



### Sumario

#### II Actos no legislativos

##### REGLAMENTOS

Reglamento de Ejecución (UE) 2015/434 de la Comisión, de 16 de marzo de 2015, por el que se establecen valores de importación a tanto alzado para la determinación del precio de entrada de determinadas frutas y hortalizas .....	1
--	---

##### DECISIONES

★ Decisión (UE) 2015/435 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2014, relativa a la movilización del Margen para Imprevistos .....	4
★ Decisión (UE) 2015/436 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2014, sobre la movilización del Fondo de Solidaridad de la Unión Europea .....	6
★ Decisión (UE) 2015/437 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2014, relativa a la movilización del Fondo de Solidaridad de la Unión Europea .....	7
★ Decisión (UE) 2015/438 del Consejo, de 2 de marzo de 2015, por la que se establece la posición que se ha de adoptar en nombre de la Unión Europea en el Comité Mixto instituido con arreglo al Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados, en lo que se refiere a la adopción de directrices comunes para la aplicación del Acuerdo .....	8
★ Decisión (PESC) 2015/439 del Consejo, de 16 de marzo de 2015, por la que se prorroga el mandato del Representante Especial de la Unión Europea para el Sahel .....	27
★ Decisión (PESC) 2015/440 del Consejo, de 16 de marzo de 2015, por la que se prorroga el mandato del Representante Especial de la Unión Europea para el Cuerno de África .....	32
★ Decisión (PESC) 2015/441 del Consejo, de 16 de marzo de 2015, por la que se modifica y prorroga la Decisión 2010/96/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas de seguridad somalíes .....	37

★ Decisión (PESC) 2015/442 del Consejo, de 16 de marzo de 2015, por la que se inicia una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUMAM RCA), y se modifica la Decisión (PESC) 2015/78 .....	39
★ Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión .....	41
★ Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE .....	53

## II

(Actos no legislativos)

## REGLAMENTOS

## REGLAMENTO DE EJECUCIÓN (UE) 2015/434 DE LA COMISIÓN

de 16 de marzo de 2015

**por el que se establecen valores de importación a tanto alzado para la determinación del precio de entrada de determinadas frutas y hortalizas**

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n° 1308/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, por el que se crea la organización común de mercados de los productos agrarios y por el que se derogan los Reglamentos (CEE) n° 922/72, (CEE) n° 234/79, (CE) n° 1037/2001 y (CE) n° 1234/2007 <sup>(1)</sup>,

Visto el Reglamento de Ejecución (UE) n° 543/2011 de la Comisión, de 7 de junio de 2011, por el que se establecen disposiciones de aplicación del Reglamento (CE) n° 1234/2007 del Consejo en los sectores de las frutas y hortalizas y de las frutas y hortalizas transformadas <sup>(2)</sup>, y, en particular, su artículo 136, apartado 1,

Considerando lo siguiente:

- (1) El Reglamento de Ejecución (UE) n° 543/2011 establece, en aplicación de los resultados de las negociaciones comerciales multilaterales de la Ronda Uruguay, los criterios para que la Comisión fije los valores de importación a tanto alzado de terceros países correspondientes a los productos y períodos que figuran en el anexo XVI, parte A, de dicho Reglamento.
- (2) De acuerdo con el artículo 136, apartado 1, del Reglamento de Ejecución (UE) n° 543/2011, el valor de importación a tanto alzado se calcula cada día hábil teniendo en cuenta datos que varían diariamente. Por lo tanto, el presente Reglamento debe entrar en vigor el día de su publicación en el *Diario Oficial de la Unión Europea*.

HA ADOPTADO EL PRESENTE REGLAMENTO:

*Artículo 1*

En el anexo del presente Reglamento quedan fijados los valores de importación a tanto alzado a que se refiere el artículo 136 del Reglamento de Ejecución (UE) n° 543/2011.

<sup>(1)</sup> DO L 347 de 20.12.2013, p. 671.

<sup>(2)</sup> DO L 157 de 15.6.2011, p. 1.

*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 2015.

*Por la Comisión,  
en nombre del Presidente,  
Jerzy PLEWA  
Director General de Agricultura y Desarrollo Rural*

---

## ANEXO

**Valores de importación a tanto alzado para la determinación del precio de entrada de determinadas frutas y hortalizas**

(EUR/100 kg)

Código NC	Código tercer país <sup>(1)</sup>	Valor de importación a tanto alzado	
0702 00 00	EG	65,8	
	MA	84,9	
	TR	86,4	
	ZZ	79,0	
0707 00 05	JO	229,9	
	MA	183,9	
	TR	185,1	
	ZZ	199,6	
0709 93 10	MA	119,5	
	TR	192,4	
	ZZ	156,0	
0805 10 20	EG	45,8	
	IL	72,7	
	MA	56,7	
	TN	57,3	
	TR	63,6	
	ZZ	59,2	
	ZZ	59,2	
0805 50 10	TR	61,4	
	ZZ	61,4	
0808 10 80	BR	70,9	
	CA	81,0	
	CL	100,9	
	CN	91,1	
	MK	25,2	
	US	166,1	
	ZZ	89,2	
	0808 30 90	AR	112,0
		CL	133,2
US		124,8	
ZA		103,5	
ZZ		118,4	

<sup>(1)</sup> Nomenclatura de países fijada por el Reglamento (UE) n° 1106/2012 de la Comisión, de 27 de noviembre de 2012, por el que se aplica el Reglamento (CE) n° 471/2009 del Parlamento Europeo y del Consejo, sobre estadísticas comunitarias relativas al comercio exterior con terceros países, en lo que concierne a la actualización de la nomenclatura de países y territorios (DO L 328 de 28.11.2012, p. 7). El código «ZZ» significa «otros orígenes».

## DECISIONES

**DECISIÓN (UE) 2015/435 DEL PARLAMENTO EUROPEO Y DEL CONSEJO  
de 17 de diciembre de 2014  
relativa a la movilización del Margen para Imprevistos**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Acuerdo Interinstitucional, de 2 de diciembre de 2013, entre el Parlamento Europeo, el Consejo y la Comisión sobre disciplina presupuestaria, cooperación en materia presupuestaria y buena gestión financiera <sup>(1)</sup>, y, en particular, su punto 14,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

- (1) El artículo 13 del Reglamento (UE, Euratom) n° 1311/2013 del Consejo <sup>(2)</sup> ha establecido un Margen para Imprevistos de hasta el 0,03 % de la renta nacional bruta de la Unión.
- (2) De conformidad con el artículo 6 de ese Reglamento, la Comisión ha calculado el importe absoluto del Margen para Imprevistos para 2014 <sup>(3)</sup>.
- (3) Después de haber examinado todas las demás posibilidades financieras para responder a las circunstancias imprevistas que han surgido después de que se fijara por primera vez, en febrero de 2013, el techo de pagos del marco financiero plurianual para 2014, resulta necesario movilizar el Margen para Imprevistos para complementar los créditos de pago en el presupuesto general de la Unión Europea para el ejercicio 2014 por encima del techo de pagos.
- (4) Debe incluirse un importe de 350 millones EUR en créditos de pago en la movilización del Margen para Imprevistos pendiente de un acuerdo sobre los pagos en relación con otros instrumentos especiales.
- (5) Vista la situación tan especial que se ha dado este año, se cumple la condición de último recurso contemplada en el artículo 13, apartado 1, del Reglamento (UE, Euratom) n° 1311/2013.
- (6) Para asegurar el cumplimiento del artículo 13, apartado 3, del Reglamento (UE, Euratom) n° 1311/2013, la Comisión debe presentar una propuesta sobre la compensación de los importes pertinentes en los techos de pago del MFP para uno o más ejercicios futuros, visto el acuerdo sobre los pagos en relación con otros instrumentos especiales y sin perjuicio de las prerrogativas institucionales de la Comisión.

<sup>(1)</sup> DO C 373 de 20.12.2013, p. 1.

<sup>(2)</sup> Reglamento (UE, Euratom) n° 1311/2013 del Consejo, de 2 de diciembre de 2013, por el que se establece el marco financiero plurianual para el período 2014-2020 (DO L 347 de 20.12.2013, p. 884).

<sup>(3)</sup> Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 20 de diciembre de 2013, relativa al ajuste técnico del marco financiero para 2014 de conformidad con las variaciones de la renta nacional bruta [COM(2013) 928].

HAN ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

En el presupuesto general de la Unión Europea para el ejercicio 2014, el Margen para Imprevistos se utilizará para poner a disposición un importe de 3 168 233 715 EUR en créditos de pago por encima del techo de pagos del marco financiero plurianual.

*Artículo 2*

La suma de 2 818 233 715 EUR se compensará en tres plazos con los márgenes existentes en los techos de pagos para los años siguientes:

- a) 2018: 939 411 200 EUR;
- b) 2019: 939 411 200 EUR;
- c) 2020: 939 411 315 EUR.

Se invita a la Comisión a que presente a su debido tiempo una propuesta sobre el importe pendiente de 350 millones EUR.

*Artículo 3*

La presente Decisión se publicará en el *Diario Oficial de la Unión Europea*.

Hecho en Estrasburgo, el 17 de diciembre de 2014.

*Por el Parlamento Europeo*

*El Presidente*

M. SCHULZ

*Por el Consejo*

*El Presidente*

B. DELLA VEDOVA

---

**DECISIÓN (UE) 2015/436 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**  
**de 17 de diciembre de 2014**  
**sobre la movilización del Fondo de Solidaridad de la Unión Europea**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) n° 2012/2002 del Consejo, de 11 de noviembre de 2002, por el que se crea el Fondo de Solidaridad de la Unión Europea <sup>(1)</sup>, y, en particular, su artículo 4, apartado 3,

Visto el Acuerdo interinstitucional, de 2 de diciembre de 2013, entre el Parlamento Europeo, el Consejo y la Comisión sobre disciplina presupuestaria, cooperación en materia presupuestaria y buena gestión financiera <sup>(2)</sup>, y, en particular, su apartado 11,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

- (1) La Unión Europea ha creado un Fondo de Solidaridad de la Unión Europea («el Fondo») para solidarizarse con la población de las regiones afectadas por catástrofes.
- (2) El artículo 10 del Reglamento (UE, Euratom) n° 1311/2013 del Consejo <sup>(3)</sup>, permite la movilización del Fondo hasta un límite máximo anual de 500 millones EUR (a precios de 2011).
- (3) El Reglamento (CE) n° 2012/2002 contiene las disposiciones que rigen la movilización del Fondo.
- (4) Italia ha presentado una solicitud de movilización del Fondo por motivo de inundaciones.
- (5) Grecia ha presentado una solicitud de movilización del Fondo por motivo de un terremoto.
- (6) Eslovenia ha presentado una solicitud de movilización del Fondo por motivo de tormentas de hielo.
- (7) Croacia ha presentado una solicitud de movilización del Fondo por motivo de tormentas de hielo seguidas de inundaciones.

HAN ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

En el marco del presupuesto general de la Unión Europea para el ejercicio presupuestario 2014, se movilizará una suma de 46 998 528 EUR en créditos de compromiso con cargo al Fondo de Solidaridad de la Unión Europea.

En el marco del presupuesto general de la Unión Europea para el ejercicio presupuestario 2015, se movilizará una suma de 46 998 528 EUR en créditos de pago con cargo al Fondo de Solidaridad de la Unión Europea.

*Artículo 2*

La presente Decisión se publicará en el *Diario Oficial de la Unión Europea*.

Hecho en Estrasburgo el 17 de diciembre de 2014.

*Por el Parlamento Europeo*

*El Presidente*

M. SCHULZ

*Por el Consejo*

*El Presidente*

B. DELLA VEDOVA

<sup>(1)</sup> DO L 311 de 14.11.2002, p. 3.

<sup>(2)</sup> DO C 373 de 20.12.2013, p. 1.

<sup>(3)</sup> Reglamento (UE, Euratom) n° 1311/2013 del Consejo, de 2 de diciembre de 2013, por el que se establece el marco financiero plurianual para el período 2014-2020 (DO L 347 de 20.12.2013, p. 884).



**DECISIÓN (UE) 2015/437 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**  
**de 17 de diciembre de 2014**  
**relativa a la movilización del Fondo de Solidaridad de la Unión Europea**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) n° 2012/2002 del Consejo, de 11 de noviembre de 2002, por el que se crea el Fondo de Solidaridad de la Unión Europea <sup>(1)</sup>, y, en particular su artículo 4, apartado 3,

Visto el Acuerdo interinstitucional, de 2 de diciembre de 2013, entre el Parlamento Europeo, el Consejo y la Comisión sobre disciplina presupuestaria, cooperación en materia presupuestaria y buena gestión financiera <sup>(2)</sup>, y, en particular su punto 11,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

- (1) La Unión Europea creó un Fondo de Solidaridad de la Unión Europea (en lo sucesivo, «el Fondo») para mostrar su solidaridad con la población de las regiones afectadas por catástrofes.
- (2) El artículo 10 del Reglamento (UE, Euratom) n° 1311/2013 del Consejo <sup>(3)</sup> permite la movilización del Fondo hasta un límite máximo anual de 50 000 000 EUR (a precios de 2011).
- (3) El Reglamento (CE) n° 2012/2002 contiene las disposiciones que rigen la movilización del Fondo.
- (4) Serbia ha presentado una solicitud de movilización del Fondo en relación con inundaciones.
- (5) Croacia ha presentado una solicitud de movilización del Fondo en relación con inundaciones.
- (6) Bulgaria ha presentado una solicitud de movilización del Fondo en relación con inundaciones.

HAN ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

En el marco del presupuesto general de la Unión Europea para el ejercicio 2014, se movilizará el Fondo de Solidaridad por un importe de 79 726 440 EUR en créditos de compromiso.

En el marco del presupuesto general de la Unión Europea para el ejercicio 2015, se movilizará el Fondo de Solidaridad por un importe de 79 726 440 EUR en créditos de pago.

*Artículo 2*

La presente Decisión se publicará en el *Diario Oficial de la Unión Europea*.

Hecho en Estrasburgo, el 17 de diciembre de 2014.

*Por el Parlamento Europeo*  
*El Presidente*  
M. SCHULZ

*Por el Consejo*  
*El Presidente*  
B. DELLA VEDOVA

<sup>(1)</sup> DO L 311 de 14.11.2002, p. 3.

<sup>(2)</sup> DO C 373 de 20.12.2013, p. 1.

<sup>(3)</sup> Reglamento (UE, Euratom) n° 1311/2013 del Consejo, de 2 de diciembre de 2013, por el que se establece el marco financiero plurianual para el período 2014-2020 (DO L 347 de 20.12.2013, p. 884).

**DECISIÓN (UE) 2015/438 DEL CONSEJO****de 2 de marzo de 2015**

**por la que se establece la posición que se ha de adoptar en nombre de la Unión Europea en el Comité Mixto instituido con arreglo al Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados, en lo que se refiere a la adopción de directrices comunes para la aplicación del Acuerdo**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 77, apartado 2, letra a), leído en relación con su artículo 218, apartado 9,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

- (1) El artículo 12 del Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados <sup>(1)</sup> («el Acuerdo») instituye un Comité Mixto. En él se establece que el Comité Mixto debe, en particular, hacer un seguimiento de la aplicación del Acuerdo.
- (2) El Acuerdo entre la Unión Europea y Ucrania por el que se modifica el Acuerdo entre la Comunidad Europea y Ucrania sobre la facilitación de la expedición de visados <sup>(2)</sup> («el Acuerdo modificador») entró en vigor el 1 de julio de 2013.
- (3) El Reglamento (CE) n° 810/2009 del Parlamento Europeo y del Consejo <sup>(3)</sup> estableció los procedimientos y condiciones para la expedición de visados de tránsito o para estancias previstas en el territorio de los Estados miembros no superiores a noventa días en un período de ciento ochenta días.
- (4) En el marco de su cometido, el Comité Mixto tomó nota de la necesidad de disponer de directrices comunes con el fin de garantizar una aplicación plenamente armonizada del Acuerdo entre los consulados de los Estados miembros, así como de aclarar la relación entre las disposiciones del Acuerdo y las disposiciones de las Partes contratantes que siguen siendo aplicables a cuestiones en materia de visados no reguladas por el Acuerdo.
- (5) El Comité Mixto adoptó tales directrices el 25 de noviembre de 2009 mediante su Decisión n° 1/2009. Dichas directrices deben adaptarse a las nuevas disposiciones del Acuerdo introducidas por el Acuerdo modificador y a los cambios en el Derecho interno de la Unión sobre la política de visados. En aras de la claridad, procede sustituir esas directrices.
- (6) Procede establecer la posición que se ha de adoptar en nombre de la Unión en el Comité Mixto en lo que se refiere a la adopción de las directrices comunes para la aplicación del Acuerdo.

HA ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

La posición que se ha de adoptar en nombre de la Unión en el Comité Mixto instituido por el artículo 12 del Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados en lo que se refiere a la adopción de directrices comunes para la aplicación del Acuerdo se basará en el proyecto de Decisión del Comité Mixto adjunto a la presente Decisión.

<sup>(1)</sup> DO L 332 de 18.12.2007, p. 68.

<sup>(2)</sup> DO L 168 de 20.6.2013, p. 11.

<sup>(3)</sup> Reglamento (CE) n° 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados) (DO L 243 de 15.9.2009, p. 1).

*Artículo 2*

La presente Decisión entrará en vigor el día de su adopción.

Hecho en Bruselas, el 2 de marzo de 2015.

*Por el Consejo*  
*La Presidenta*  
D. REIZNIECE-OZOLA

\_\_\_\_\_

## PROYECTO

**DECISIÓN Nº .../2014 DEL COMITÉ MIXTO INSTITUIDO POR EL ACUERDO ENTRE LA UNIÓN EUROPEA Y UCRANIA SOBRE LA FACILITACIÓN DE LA EXPEDICIÓN DE VISADOS****de ...****en lo que se refiere a la adopción de directrices comunes para la aplicación del Acuerdo**

EL COMITÉ MIXTO,

Visto el Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados («el Acuerdo»), y en particular su artículo 12,

Considerando que el Acuerdo entró en vigor el 1 de enero de 2008,

DECIDE:

*Artículo 1*

Se establecen en el anexo de la presente Decisión las Directrices comunes para la aplicación del Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados.

*Artículo 2*

Queda derogada la Decisión nº 1/2009 del Comité Mixto.

*Artículo 3*

La presente Decisión entrará en vigor el día de su adopción.

Hecho en ..., el

*Por la Unión Europea**Por Ucrania*

\_\_\_\_\_

## ANEXO

**DIRECTRICES COMUNES PARA LA APLICACIÓN DEL ACUERDO ENTRE LA UNIÓN EUROPEA Y  
UCRANIA SOBRE LA FACILITACIÓN DE LA EXPEDICIÓN DE VISADOS**

El Acuerdo entre la Unión Europea y Ucrania sobre la facilitación de la expedición de visados, que entró en vigor el 1 de enero de 2008, modificado por el Acuerdo entre la Unión Europea y Ucrania de 23 de julio de 2012, que entró en vigor el 1 de julio de 2013 («el Acuerdo»), tiene por objeto facilitar, sobre una base de reciprocidad, los procedimientos de expedición de visados para estancias cuya duración prevista no exceda de los noventa días por período de ciento ochenta días a los ciudadanos de Ucrania.

El Acuerdo establece, sobre una base de reciprocidad, derechos y obligaciones jurídicamente vinculantes con el fin de simplificar los procedimientos de expedición de visados para los ciudadanos ucranianos.

Las presentes Directrices, adoptadas por el Comité Mixto instituido por el artículo 12 del Acuerdo («el Comité Mixto»), tienen por objeto garantizar una aplicación correcta y armonizada de las disposiciones del Acuerdo por las misiones diplomáticas y oficinas consulares de los Estados miembros. Las presentes Directrices no forman parte del Acuerdo y no son, por tanto, jurídicamente vinculantes. Sin embargo, se recomienda encarecidamente que el personal diplomático y consular las siga consistentemente a la hora de aplicar las disposiciones del Acuerdo.

Se prevé que las presentes Directrices se actualicen a la luz de la experiencia adquirida en la aplicación del Acuerdo bajo la responsabilidad del Comité Mixto. Las Directrices, adoptadas por el Comité mixto el 25 de noviembre de 2009, se han adaptado en consonancia con el Acuerdo entre la Unión Europea y Ucrania por el que se modifica el Acuerdo entre la Comunidad Europea y Ucrania sobre la facilitación de la expedición de visados («el Acuerdo modificador»), y con la nueva legislación de la Unión, como el Reglamento (CE) n° 810/2009 del Parlamento Europeo y del Consejo <sup>(1)</sup> («Código de visados»).

**I. CUESTIONES GENERALES.****1.1. Objeto y ámbito de aplicación.**

EL artículo 1 del Acuerdo dispone lo siguiente: «El presente Acuerdo tiene por objeto facilitar la expedición de visados a los ciudadanos de Ucrania para estancias cuya duración prevista no exceda de los 90 días por período de 180 días.»

El Acuerdo se aplica a todos los ciudadanos ucranianos que soliciten un visado de corta duración, con independencia del país en el que residan.

El artículo 1, apartado 2, del Acuerdo dispone lo siguiente: «Ucrania solo podrá reintroducir la obligación de visado para los ciudadanos o determinadas categorías de ciudadanos de todos los Estados miembros y no para los ciudadanos o determinadas categorías de ciudadanos de Estados miembros concretos. Si Ucrania reintrodujera la obligación de solicitar visado para los ciudadanos de la Unión Europea o determinadas categorías de ellos, las mismas facilidades otorgadas a los ciudadanos ucranianos en aplicación del presente Acuerdo se aplicarían de forma automática y recíproca a los ciudadanos de la Unión Europea.»

Conforme a las decisiones adoptadas por el Gobierno ucraniano, desde el 1 de mayo de 2005 o del 1 de enero de 2008, respectivamente, los ciudadanos de la Unión están exentos de la obligación de visado cuando viajen a Ucrania por un período de tiempo no superior a noventa días o transiten por el territorio de ese país. Esta disposición no afecta al derecho del Gobierno ucraniano a modificar dichas decisiones.

**1.2. Ámbito de aplicación del Acuerdo.**

El artículo 2 del Acuerdo dispone lo siguiente:

«1. Las medidas destinadas a facilitar la expedición de visados contempladas en el presente Acuerdo se aplicarán a los ciudadanos de Ucrania únicamente en la medida en que estos no estén exentos de la obligación de visado en virtud de las disposiciones legales y reglamentarias de la Unión Europea o sus Estados miembros, del presente Acuerdo o de otros acuerdos internacionales.

2. El Derecho nacional de Ucrania o de los Estados miembros, o el Derecho de la Unión Europea se aplicarán a las cuestiones que no estén reguladas por las disposiciones del presente Acuerdo, como la negativa a expedir un visado, el reconocimiento de los documentos de viaje, la prueba de la existencia de medios de subsistencia suficientes, la denegación de entrada y las medidas de expulsión.»

<sup>(1)</sup> Reglamento (CE) n° 810/2009 del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados) (DO L 243 de 15.9.2009, p. 1).

Sin perjuicio de lo dispuesto en su artículo 10 (que prevé la exención de la obligación de visado para los titulares de pasaportes diplomáticos y pasaportes de servicio biométricos de Ucrania), el Acuerdo no afecta a las normas vigentes sobre las obligaciones de visado y las exenciones de visado. Por ejemplo, el artículo 4 del Reglamento (CE) nº 539/2001 <sup>(1)</sup> del Consejo autoriza a los Estados miembros a eximir de la obligación de visado a la tripulación civil de aviones y buques, entre otras categorías.

La normativa de Schengen y, cuando proceda, el Derecho nacional seguirán aplicándose a las cuestiones que no estén reguladas por el Acuerdo, como la negativa a expedir un visado, el reconocimiento de los documentos de viaje, la prueba de la existencia de unos medios de subsistencia suficientes, la denegación de entrada y las medidas de expulsión. Esto se aplica también a la normativa de Schengen que determina cuál es el Estado miembro Schengen responsable de tramitar una solicitud de visado. Por consiguiente, los ciudadanos ucranianos deberán seguir solicitando un visado en el consulado del Estado miembro del destino principal de su viaje; si no existe un destino principal, deberán presentar la solicitud en la oficina consular del Estado miembro de la primera entrada en el espacio Schengen.

Incluso en el caso de que se cumplan las condiciones previstas en el Acuerdo, por ejemplo que el solicitante de visado aporte pruebas documentales de la finalidad del viaje para las categorías previstas en el artículo 4, es posible que le sea denegada la expedición del visado si no se cumplen las condiciones previstas en el artículo 5 del Reglamento (CE) nº 562/2006 del Parlamento Europeo y del Consejo <sup>(2)</sup> («Código de fronteras Schengen»), es decir, que la persona no esté en posesión de un documento de viaje válido, se haya expedido una descripción en el SIS, se considere que la persona constituye una amenaza para el orden público, la seguridad interior, etc.

Seguirán siendo válidas las otras posibilidades de flexibilidad en la expedición de visados contempladas en el Código de visados. Por ejemplo, podrán expedirse visados de entradas múltiples con un período de validez prolongado —hasta cinco años— a categorías de personas distintas de las contempladas en el artículo 5 del Acuerdo, siempre que se cumplan las condiciones previstas en el Código de visados (véase el artículo 24, apartado 2, del Código de visados). De la misma manera, seguirán siendo aplicables las disposiciones recogidas en el Código de visados que permiten la exención o la reducción de las tasas de visado (véase el punto II.2.1.1).

### 1.3. Tipos de visados que entran en el ámbito de aplicación del Acuerdo.

El artículo 3, letra d), del Acuerdo define el «visado» como «una autorización o permiso expedidos por un Estado miembro o una decisión adoptada por dicho Estado que se precise para:

- entrar en dicho Estado o en varios Estados miembros para una estancia cuya duración prevista no exceda de los 90 días,
- entrar a efectos de tránsito en el territorio de ese Estado miembro o de varios Estados miembros.».

El Acuerdo abarca el siguiente tipo de visados:

- visados de categoría C (visados para estancias de corta duración).

Las facilidades previstas en el Acuerdo se aplican tanto a los visados uniformes válidos para todo el territorio de los Estados miembros como a los visados de validez territorial limitada (VTL).

### 1.4. Cálculo de la duración de la estancia autorizada por un visado y, en particular, la cuestión sobre cómo determinar el período de seis meses.

La reciente modificación del Código de fronteras Schengen ha redefinido el concepto de estancia de corta duración. La definición actual reza así: «90 días dentro de cualquier período de 180 días, lo que implica tener en cuenta el período de 180 días que precede a cada día de estancia».

Se entenderá por día de entrada el primer día de estancia en el territorio de los Estados miembros, y por día de salida, el último día de estancia en el territorio de los Estados miembros. El concepto de «cualquier» supone la aplicación de un período de referencia de ciento ochenta días «movible», mirando retrospectivamente cada día de la estancia al último período de ciento ochenta días, con el fin de comprobar si sigue cumpliéndose el requisito de noventa/ciento ochenta días. Ello significa que una ausencia durante un período ininterrumpido de noventa días permite una nueva estancia de hasta noventa días.

La definición entró en vigor el 18 de octubre de 2013. La calculadora puede encontrarse en línea, en la siguiente dirección: [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm).

<sup>(1)</sup> Reglamento (CE) nº 539/2001 del Consejo, de 15 de marzo de 2001, por el que se establecen la lista de terceros países cuyos nacionales están sometidos a la obligación de visado para cruzar las fronteras exteriores y la lista de terceros países cuyos nacionales están exentos de esa obligación (DO L 81 de 21.3.2001, p. 1).

<sup>(2)</sup> Reglamento (CE) nº 562/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen) (DO L 105 de 13.4.2006, p. 1).

Ejemplo de cálculo de la estancia sobre la base de la nueva definición:

El titular de un visado para entradas múltiples con un período de validez de un año (del 18 de abril de 2014 al 18 de abril de 2015) entra por primera vez el 19 de abril de 2014 y permanece tres días. Posteriormente vuelve a entrar el 18 de junio de 2014 y permanece ochenta y seis días. ¿Cuál es la situación en fechas específicas? ¿Cuándo se le autorizará a entrar de nuevo?

El 11 de septiembre de 2014: a lo largo de los últimos ciento ochenta días (del 16 de marzo de 2014 al 11 de septiembre de 2014) la persona ha permanecido tres días (del 19 al 21 de abril de 2014), más ochenta y seis días (del 18 de junio al 11 de septiembre de 2014) = ochenta y nueve días = No se ha sobrepasado el período de estancia autorizado. La persona puede permanecer aún un día más.

A partir del 16 de octubre de 2014: la persona puede entrar para una estancia de tres días adicionales [el 16 de octubre de 2014, la estancia del 19 de abril de 2014 deja de ser pertinente (fuera del período de ciento ochenta días)]; el 17 de octubre de 2014, la estancia del 20 de abril de 2014 deja de ser pertinente (fuera del período de ciento ochenta días; etc.).

A partir del 15 de diciembre de 2014: la persona puede entrar para una estancia de ochenta y seis días adicionales [el 15 de diciembre de 2014, la estancia del 18 de junio de 2014 deja de ser pertinente (fuera del período de ciento ochenta días); el 16 de diciembre de 2014, la estancia del 19 de junio de 2014 deja de ser pertinente, etc.].

#### **1.5. Situación en lo que respecta a los Estados miembros que todavía no aplican plenamente el acervo de Schengen, los Estados miembros que no participan en la política común de visados de la UE y los países asociados.**

Los Estados miembros que se adhirieron a la Unión en 2004 (República Checa, Estonia, Chipre, Letonia, Lituania, Hungría, Malta, Polonia, Eslovenia y Eslovaquia), 2007 (Bulgaria y Rumanía) y 2013 (Croacia) están vinculados por el Acuerdo a partir de su entrada en vigor.

Solo Bulgaria, Croacia, Chipre y Rumanía aún no aplican plenamente el acervo de Schengen. Seguirán expidiendo visados nacionales con una validez limitada a su propio territorio nacional. Una vez que esos Estados miembros apliquen plenamente el acervo de Schengen, seguirán aplicando el Acuerdo.

El Derecho nacional sigue siendo aplicable a todas las cuestiones que no estén reguladas por el Acuerdo, hasta la fecha de plena aplicación del acervo de Schengen por parte de esos Estados miembros. A partir de esa fecha la normativa Schengen/el Derecho nacional será aplicable a las cuestiones no reguladas por el Acuerdo.

Bulgaria, Chipre, Croacia, y Rumanía están autorizados a reconocer los permisos de residencia, los visados D y los visados para estancias de corta duración expedidos por los Estados Schengen y los países asociados para estancias de corta duración en sus territorios.

De conformidad con el artículo 21 del Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 relativo a la supresión gradual de los controles en las fronteras comunes, todos los Estados Schengen deben reconocer los visados para estancias de larga duración y los permisos de residencia expedidos por cada uno de ellos como válidos para estancias de corta duración en los territorios de los demás. Los Estados miembros Schengen aceptan los permisos de residencia, los visados D y los visados para estancias de corta duración de países asociados a efectos de entrada y estancia de corta duración, y viceversa.

El Acuerdo no se aplica a Dinamarca, Irlanda y el Reino Unido, pero incluye declaraciones conjuntas sobre la conveniencia de que esos Estados miembros celebren acuerdos bilaterales sobre la facilitación de la expedición de visados con Ucrania.

El 1 de marzo de 2009 entró en vigor un acuerdo bilateral sobre la facilitación de la expedición de visados entre Dinamarca y Ucrania. No ha habido negociaciones sobre la facilitación de visados entre Ucrania y, respectivamente, Irlanda y el Reino Unido.

Aunque asociados a Schengen, el Acuerdo no se aplica a Islandia, Liechtenstein, Noruega y Suiza, pero incluye declaraciones conjuntas sobre la conveniencia de que esos países Schengen celebren acuerdos bilaterales sobre la facilitación de la expedición de visados con Ucrania.

El 13 de febrero de 2008, Noruega firmó un acuerdo bilateral sobre la facilitación de la expedición de visados. Ese Acuerdo entró en vigor el 1 de septiembre de 2011.

Suiza concluyó las negociaciones sobre un acuerdo bilateral de facilitación de la expedición de visados en noviembre de 2011. Islandia ha indicado que han comenzado las negociaciones con Ucrania.

#### **1.6. El Acuerdo/Acuerdos bilaterales.**

El artículo 13, apartado 1, del Acuerdo dispone lo siguiente:

«1. Desde el momento de su entrada en vigor, el presente Acuerdo prevalecerá sobre las disposiciones de cualquier convenio o acuerdo bilateral o multilateral celebrado entre los distintos Estados miembros y Ucrania, en la medida en que tales disposiciones aborden cuestiones reguladas por el presente Acuerdo.».

A partir de la fecha de entrada en vigor del Acuerdo, las disposiciones de los acuerdos bilaterales en vigor entre los Estados miembros y Ucrania sobre cuestiones reguladas por el Acuerdo dejaron de ser aplicables. De conformidad con el Derecho de la Unión, los Estados miembros deben adoptar las medidas necesarias para eliminar las incompatibilidades entre sus acuerdos bilaterales y el Acuerdo.

No obstante, el artículo 13, apartado 2, del Acuerdo dispone lo siguiente:

«2. Las disposiciones de los acuerdos o convenios bilaterales entre los distintos Estados miembros y Ucrania celebrados antes de la entrada en vigor del presente Acuerdo que prevean la exención de la obligación de visado para los titulares de pasaportes de servicio no biométricos seguirán aplicándose, sin perjuicio del derecho de los Estados miembros afectados o de Ucrania de denunciar o suspender dichos acuerdos o convenios bilaterales.»

Los siguientes Estados miembros han firmado un acuerdo bilateral con Ucrania que prevé la exención de la obligación de visado para los titulares de pasaportes de servicio: Bulgaria, Chipre, Croacia, Eslovaquia, Letonia, Lituania, Hungría, Polonia y Rumanía.

De conformidad con el artículo 13, apartado 1, del Acuerdo, en la medida en que estos acuerdos bilaterales se apliquen a los titulares de pasaportes de servicio biométricos, el artículo 10, apartado 2, del Acuerdo prevalece sobre dichos acuerdos bilaterales. De conformidad con el artículo 13, apartado 2, del Acuerdo, aquellos acuerdos bilaterales celebrados antes de la entrada en vigor del Acuerdo modificador siguen siendo de aplicación en la medida en que atañen a los titulares de pasaportes de servicio no biométricos, sin perjuicio del derecho de los Estados miembros afectados o de Ucrania a denunciar o suspender dichos acuerdos o convenios bilaterales. La exención de la obligación de visado para los titulares de pasaportes de servicio no biométricos concedida por un Estado miembro solo se aplica para desplazarse en el territorio de ese Estado miembro y no para viajar a los demás Estados miembros Schengen.

Si un Estado miembro hubiera celebrado un acuerdo o convenio bilateral con Ucrania sobre cuestiones no reguladas por el Acuerdo, esta exención seguiría aplicándose tras la entrada en vigor del Acuerdo.

#### **1.7. Declaración de la Comunidad Europea relativa al acceso de los solicitantes de visados y a la armonización de la información sobre los procedimientos de expedición de visados de corta duración y sobre los documentos que deben facilitarse en apoyo de una solicitud de visado de corta duración.**

De conformidad con dicha Declaración de la Comunidad Europea aneja al Acuerdo, la información básica común relativa al acceso de los solicitantes de visado a las misiones diplomáticas y las oficinas consulares de los Estados miembros, sobre los procedimientos y los requisitos para la obtención de visados y sobre la validez de los visados expedidos se ha establecido para garantizar que los solicitantes reciban una información coherente y uniforme. Dicha información está disponible en la página web de la Delegación de la UE en Ucrania: [http://eeas.europa.eu/delegations/ukraine/index\\_en.htm](http://eeas.europa.eu/delegations/ukraine/index_en.htm).

Las misiones diplomáticas y oficinas consulares de los Estados miembros deben dar amplia difusión a esta información (utilizando los tableros de anuncios, en forma de folletos, a través de internet, etc.) y facilitar información precisa sobre las condiciones para la expedición de visados, la representación de los Estados miembros en Ucrania y la lista armonizada de la UE de documentos justificativos requeridos.

## **II. DIRECTRICES SOBRE DISPOSICIONES ESPECÍFICAS.**

### **2.1. Normas que se aplican a todos los solicitantes de visado**

Importante: Se recuerda que las facilidades que se mencionan a continuación en lo que se refiere a las tasas de tramitación de visados, la duración de los procedimientos de tramitación de las solicitudes de visado, la salida en caso de pérdida o robo de documentos y la prórroga del visado en circunstancias excepcionales se aplican a todos los solicitantes de visados y titulares de visados ucranianos.

#### *2.1.1. Tasas de tramitación de visados.*

El artículo 6, apartado 1, del Acuerdo dispone lo siguiente:

«La tasa aplicada a la tramitación de las solicitudes de visado presentadas por ciudadanos ucranianos será de 35 EUR. Este importe podrá revisarse en aplicación del procedimiento previsto en el artículo 14, apartado 4.»

De conformidad con el artículo 6, apartado 1, la tasa aplicada a la tramitación de una solicitud de visado es de 35 EUR. Esta tasa se aplicará a todos los solicitantes de visados ucranianos (incluidos los turistas) y atañe a los visados de corta duración, con independencia del número de entradas. También se aplica a las solicitudes de visado presentadas en las fronteras exteriores.

El artículo 6, apartado 2, del Acuerdo dispone lo siguiente:

«Si Ucrania reintrodujera la obligación de visado para los ciudadanos de la UE, la tasa que Ucrania exigiría por la expedición de visado no superaría los 35 EUR o el importe que se acuerde, si la tasa se revisara de conformidad con el procedimiento establecido en el artículo 14, apartado 4.»



El artículo 6, apartado 3, del Acuerdo dispone lo siguiente:

«Los Estados miembros cobrarán una tasa de 70 EUR por la tramitación de un visado cuando, debido a la distancia entre el lugar de residencia del solicitante y el lugar en que se ha presentado la solicitud, el solicitante pida que la decisión sobre su solicitud se adopte en un plazo de tres días a partir de la presentación de la misma, y el consulado acepte adoptar una decisión en este plazo».

Se cobrará una tasa de 70 EUR por la tramitación de las solicitudes de visado en caso de que la solicitud de visado y los documentos justificativos hayan sido presentados por un solicitante de visado cuyo lugar de residencia se encuentre en una región en la que el Estado miembro al que el solicitante desee viajar no tenga una representación consular (si en dicha región no existe ningún consulado, ni centro de visados, ni consulados de los Estados miembros que han concluido acuerdos de representación con el Estado miembro al que el solicitante desea viajar), y cuando la misión diplomática o la oficina consular hayan acordado adoptar una decisión sobre la solicitud de visado en el plazo de tres días. En el impreso de solicitud de visado se prevén pruebas relativas al lugar de residencia del solicitante de visado.

En principio, el artículo 6, apartado 3, del Acuerdo tiene por objeto facilitar la solicitud de visado a los solicitantes que viven a gran distancia del consulado. En caso de que fuera necesario un viaje de larga duración para solicitar el visado, el objetivo es expedirlo rápidamente, de forma que el solicitante pueda recibir el visado sin necesidad de realizar el mismo largo viaje una segunda vez.

Por las razones antes mencionadas, en los casos en que el tiempo de tramitación «normal» para una solicitud de visado por una misión diplomática u oficina consular dadas sea de tres días o menos, se cobrará la tasa normal de 35 EUR.

Por lo que se refiere a las misiones diplomáticas y oficinas consulares que cuenten con un sistema de cita, el período de tiempo necesario para conseguir una cita no se contará como parte del tiempo de tramitación (véase también II.2.1.2).

El artículo 6, apartado 4, del Acuerdo dispone lo siguiente:

«4. Sin perjuicio de lo dispuesto en el apartado 5, las categorías de personas siguientes estarán exentas del pago de la tasa exigible por la tramitación de un visado:

a) los parientes cercanos, como cónyuges, hijos (incluidos los adoptivos), padres (incluidos los tutores legales), abuelos y nietos, que visiten a nacionales ucranianos que residan legalmente en el territorio de los Estados miembros o los ciudadanos de la Unión Europea que residan en el territorio del Estado miembro del que son nacionales.»

(N.B. Este punto regula la situación de los parientes cercanos ucranianos que viajen a los Estados miembros para visitar a nacionales ucranianos que residan legalmente en los Estados miembros o a ciudadanos de la Unión Europea que residan en el territorio del Estado miembro del que son nacionales. A los solicitantes ucranianos que sean parientes de un ciudadano de la Unión, en el sentido del artículo 5, apartado 2, de la Directiva 2004/38/CE del Parlamento Europeo y del Consejo <sup>(1)</sup>, los visados se les expedirán gratuitamente lo antes posible y mediante un procedimiento acelerado).

b) los miembros de delegaciones oficiales que, a raíz de una invitación oficial dirigida a Ucrania, participen en reuniones, consultas, negociaciones o programas de intercambio, o bien en eventos celebrados por organizaciones intergubernamentales en el territorio de uno de los Estados miembros;

c) los miembros de los gobiernos y parlamentos nacionales y regionales y miembros de los tribunales Constitucional y Supremo, siempre que estas personas no estén exentas de la obligación de visado en virtud del presente Acuerdo;

d) los estudiantes de los distintos ciclos, incluido el postgrado, y los profesores acompañantes que realizan viajes de estudios o con fines educativos;

e) las personas discapacitadas y, en caso necesario, sus acompañantes;» (N.B. Para poder acogerse a la exención del pago de la tasa, deberá probarse que cada uno de los solicitantes de visado entran dentro de esta categoría.)

f) las personas que hayan presentado documentos en los que se certifique la necesidad de su viaje por razones humanitarias, inclusive para recibir un tratamiento médico urgente, en cuyo caso también estarán exentos sus eventuales acompañantes, o para asistir al entierro de un pariente cercano, o para visitar a un pariente cercano gravemente enfermo;

g) los participantes en acontecimientos deportivos internacionales y sus acompañantes;» (N.B. Solo se aplica a los acompañantes que viajen a título profesional; no se considerarán acompañantes los seguidores).

<sup>(1)</sup> Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros por la que se modifica el Reglamento (CEE) nº 1612/68 y se derogan las Directivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE y 93/96/CEE (DO L 158 de 30.4.2004, p. 77).

- «h) las personas que participen en actividades científicas, culturales y artísticas, incluidos los programas de intercambio universitarios o de otro tipo;
- i) las personas que participen en programas oficiales de intercambio organizados por ciudades hermanadas y otros entes municipales;
- j) los periodistas y el personal técnico que los acompañe con fines profesionales;» (N.B. La presente letra se aplica a los periodistas contemplados en el artículo 4, apartado 1, letra e), del Acuerdo.)
- «k) los pensionistas;» (N.B. Para poder acogerse a la exención de la tasa correspondiente a esta categoría, los solicitantes de visados tendrán que acreditar su condición de pensionistas.)
- «l) los conductores que presten en vehículos matriculados en Ucrania servicios de transporte internacional de mercancías y pasajeros que tengan como destino el territorio de los Estados miembros;
- m) el personal de los vagones, vagones frigoríficos y locomotoras de los trenes internacionales que tengan como destino el territorio de los Estados miembros;
- n) los menores de 18 años y los hijos a cargo menores de 21 años.» (N.B. Para poder acogerse a la exención de la tasa dentro de esta categoría, los solicitantes de visado tendrán que acreditar su edad y —si son menores de 21 años— demostrar su dependencia.)
- «o) los representantes de comunidades religiosas;
- p) los miembros de profesiones liberales que participen en ferias, conferencias, simposios, seminarios internacionales o actos similares celebrados en el territorio de los Estados miembros;
- q) personas menores de veinticinco años que vayan a participar en seminarios, conferencias o acontecimientos deportivos, culturales o educativos, organizados por organizaciones sin ánimo de lucro;
- r) los representantes de organizaciones de la sociedad civil que se desplacen para recibir formación o participar en seminarios y conferencias, por ejemplo en el marco de programas de intercambio;
- s) los participantes en programas oficiales de cooperación transfronteriza de la Unión Europea, por ejemplo en el marco del Instrumento Europeo de Vecindad y Asociación (IEVA).

El primer párrafo se aplicará también cuando el viaje sea de tránsito.»

El artículo 6, apartado 4, párrafo segundo, del Acuerdo solo se aplica si el propósito del viaje al tercer país es equivalente a uno de los fines contemplados en el artículo 6, apartado 4, letras a) a s), del Acuerdo, por ejemplo si el tránsito es necesario para asistir a un seminario, para visitar a familiares, para participar en un programa de intercambio de organizaciones de la sociedad civil, etc. en el tercer país.

Las citadas categorías de personas están totalmente exentas del pago de la tasa. Por otro lado, conforme al artículo 16, apartado 6, del Código de visados, «en determinados casos, el importe de las tasas de visado podrá reducirse o suprimirse cuando ello sirva para fomentar intereses culturales o deportivos, o intereses en el ámbito de la política exterior, la política de desarrollo y otros ámbitos de interés público esencial o por razones humanitarias.»

Sin embargo, dicha norma no puede aplicarse para quedar eximido del pago de la tasa de 70 EUR en casos individuales, cuando la solicitud de visado y los documentos justificativos hayan sido presentados por un solicitante de visado cuyo lugar de residencia se encuentre lejos de la misión diplomática o la oficina consular del Estado miembro y que pertenezca a una de las categorías exentas del pago de las tasas de visado contempladas en el artículo 6, apartado 4, del Acuerdo.

Cabe recordar asimismo que las categorías de personas exentas del pago de las tasas de visado pueden estar sujetas a una tasa de servicio en caso de que un Estado miembro coopere con un proveedor de servicios externo.

El artículo 6, apartado 5, del Acuerdo dispone lo siguiente:

«5. Si un Estado miembro coopera con un proveedor de servicios externo a efectos de la expedición de un visado, el prestador de servicios externo podrá cobrar una tasa por el servicio prestado. Esta tasa será proporcional a los gastos en que incurra el prestador de servicios externo para la realización de sus tareas y no excederá de 30 EUR. Los Estados miembros mantendrán la posibilidad de que los solicitantes presenten sus solicitudes directamente en sus consulados. Si se exige a los solicitantes que pidan cita para la presentación de la solicitud, la cita tendrá lugar, por regla general, en el plazo de dos semanas siguientes a la fecha en que se solicitó la cita.»

Mantener la posibilidad de que todas las categorías de solicitantes de visado presenten sus solicitudes directamente en el consulado en lugar de hacerlo a través de un proveedor de servicios externo implica la existencia de una auténtica opción entre ambas posibilidades. Aunque el acceso directo no tiene que estar organizado en condiciones idénticas o similares a las del acceso al proveedor de servicios, dichas condiciones no deben imposibilitar en la práctica el acceso directo. Aunque es aceptable que el tiempo de espera para obtener una cita sea diferente en el caso de acceso directo, no debería ser tan largo como para hacer imposible en la práctica el acceso directo.

#### 2.1.2. Duración de los procedimientos de tramitación de las solicitudes de visado.

EL artículo 7 del Acuerdo dispone lo siguiente:

- «1. Las misiones diplomáticas y oficinas consulares de los Estados miembros decidirán si expiden o no un visado dentro de los diez días naturales posteriores a la recepción de la solicitud y de los documentos de acompañamiento necesarios para su expedición.
2. El plazo establecido para la adopción de una decisión sobre una solicitud de visado podrá ampliarse a treinta días naturales en casos singulares, y en particular cuando resulte necesario un examen complementario de la solicitud.
3. En caso de urgencia, el plazo establecido para la adopción de una decisión sobre una solicitud de visado podrá reducirse a dos días laborables, o incluso menos.»

La decisión sobre la solicitud de visado deberá tomarse en principio en el plazo de diez días naturales a partir de la fecha de la recepción de la solicitud de visado completa y de los documentos justificativos.

Dicho plazo podrá ampliarse a un máximo de treinta días cuando se requiera un examen complementario, por ejemplo, para consultar a las autoridades centrales.

Todos esos plazos solo empiezan a correr en el momento en que el expediente de solicitud esté completo, es decir, a partir de la fecha de recepción de la solicitud de visado y de los documentos justificativos.

En cuanto a las misiones diplomáticas y oficinas consulares que dispongan de un sistema de cita, el plazo para obtener una cita no se contará como parte del tiempo de tramitación. A la hora de fijar la cita, debe tenerse en cuenta la urgencia alegada por el solicitante de visado con vistas a la aplicación del artículo 7, apartado 3, del Acuerdo. En general, la cita debe tener lugar en un plazo de dos semanas a partir de la fecha en que se solicitó (véase el artículo 6, apartado 5, del Acuerdo). Solo excepcionalmente se debe aceptar un plazo más largo, incluso en los períodos de máxima demanda. El Comité Mixto supervisará detenidamente esta cuestión. Los Estados miembros velarán por garantizar que las citas a petición de los miembros de delegaciones oficiales de Ucrania para presentar solicitudes en las misiones diplomáticas y oficinas consulares tengan lugar tan pronto como sea posible, preferentemente en un plazo de dos días laborables, en casos urgentes, cuando la invitación se haya enviado con retraso.

La decisión sobre la reducción de los plazos para la adopción de una decisión sobre una solicitud de visado, tal como se define en el artículo 7, apartado 3, del Acuerdo, es tomada por el funcionario consular.

#### 2.1.3. Prórroga del visado en circunstancias excepcionales.

El artículo 9 del Acuerdo dispone lo siguiente:

«Para los ciudadanos de Ucrania que se hallen en la imposibilidad de abandonar el territorio de los Estados miembros en la fecha que figura en su visado por razones de fuerza mayor, se prorrogará la vigencia de su visado gratuitamente de acuerdo con la legislación aplicada por el Estado anfitrión por el plazo necesario para su regreso al Estado de residencia.»

En lo que respecta a la posibilidad de prorrogar el período de validez del visado en caso de fuerza mayor —por ejemplo, estancia en un hospital debido a razones imprevistas/enfermedad repentina/accidente— en caso de que el titular del visado no tenga la posibilidad de abandonar el territorio del Estado miembro antes de que pase la fecha fijada en el visado, las disposiciones del artículo 33, apartado 1, del Código de visados se aplicarán en la medida en que sean compatibles con el Acuerdo (por ejemplo, el visado prorrogado seguirá siendo un visado uniforme que permite la entrada al territorio de todos los Estados miembros del espacio Schengen para los que el visado era válido en el momento de la expedición). No obstante, en el marco del Acuerdo la prórroga del visado se hace de forma gratuita en caso de fuerza mayor.

## 2.2. Normas aplicables a determinadas categorías de solicitantes de visado.

### 2.2.1. Pruebas documentales del objeto del viaje

Para todas las categorías de personas mencionadas en el artículo 4, apartado 1, del Acuerdo, incluidos los conductores que lleven a cabo servicios de transporte internacional de mercancías y pasajeros, solo serán necesarias pruebas documentales relativas al propósito del viaje. En el caso de estas categorías de solicitantes, no debe exigirse ningún otro documento relativo al propósito de la estancia. Como se indica en el artículo 4, apartado 3, no será necesaria ninguna otra justificación, invitación o validación en relación con el objeto del viaje.

Si en casos particulares quedan dudas sobre el objeto real del viaje, el solicitante de visado debe ser convocado para una entrevista en profundidad (adicional) a la embajada/consulado, donde podrá ser interrogado en relación con el objeto real de la visita o la intención del solicitante de volver (véase el artículo 21, apartado 8, del Código de visados). En tales casos individuales, el solicitante de visado podrá aportar documentos complementarios, o, excepcionalmente, el funcionario consular podrá solicitarlos. El Comité Mixto supervisará de cerca esta cuestión.

Para las categorías de personas no mencionadas en el artículo 4 del Acuerdo, las normas vigentes siguen siendo de aplicación a la documentación que acredite el objeto del viaje. Lo mismo se aplica a los documentos relativos a la autorización parental de viaje de niños menores de 18 años.

A las cuestiones que no estén reguladas por las disposiciones del Acuerdo, como el reconocimiento de los documentos de viaje, el seguro médico de viaje y las garantías relativas al retorno y los medios de subsistencia suficientes, se les aplica la normativa de Schengen o el Derecho nacional (véase, I.1.2.).

En consonancia con la «Declaración de la Unión Europea sobre los documentos que deberán presentarse al solicitar el visado para estancia de corta duración», aneja al Acuerdo modificador, «la Unión Europea elaborará una lista armonizada de los documentos justificativos, de conformidad con el artículo 48, apartado 1, letra a), del Código de visados, para garantizar que a los solicitantes procedentes de Ucrania se les exija presentar, en principio, los mismos documentos justificativos»; los consulados de los Estados miembros, actuando en el marco de la cooperación local Schengen, han de velar por que los solicitantes de visados ucranianos reciban una información básica coherente y uniforme y por que se les exija presentar, en principio, los mismos documentos justificativos con independencia del consulado del Estado miembro en el que presenten la solicitud.

En principio, el original de la invitación o el certificado del documento exigidos en el artículo 4, apartado 1, del Acuerdo, se presentarán junto con la solicitud de visado. Sin embargo, el consulado puede empezar a tramitar la solicitud del visado con facsímiles o copias de la invitación o el certificado del documento. En cualquier caso, el consulado puede exigir el documento original en caso de que se trate de la primera solicitud y lo pedirá en casos concretos, cuando existan dudas.

Como las listas de autoridades que figuran a continuación también incluyen a veces el nombre de la persona que puede firmar las invitaciones/los certificados pertinentes, las autoridades ucranianas deben informar a la cooperación local en el marco de Schengen cuando se sustituya a esas personas.

El Artículo 4 del Acuerdo dispone lo siguiente:

- «1. Para las siguientes categorías de ciudadanos de Ucrania, la presentación de los documentos que se enumeran a continuación bastará para justificar ante la otra Parte el objeto del viaje:
- a) para los miembros de delegaciones oficiales que, a raíz de una invitación oficial dirigida a Ucrania, participen en reuniones, consultas, negociaciones o programas de intercambio, o bien en eventos celebrados por organizaciones intergubernamentales en el territorio de alguno de los Estados miembros:
    - una carta expedida por una autoridad ucraniana en la que se confirme que el solicitante es miembro de su delegación en viaje a la otra Parte para participar en los eventos anteriormente mencionados, junto con una copia de la invitación oficial;»

El nombre del solicitante debe indicarse en la carta expedida por la autoridad competente en la que se confirme que la persona es miembro de la delegación que viaja al territorio de la otra Parte para participar en la reunión oficial. El nombre del solicitante no tiene por qué figurar necesariamente también en la invitación oficial para participar en la reunión, si bien este podría ser el caso cuando la invitación oficial se dirige a una persona concreta.

Dicha disposición se aplica a los miembros de delegaciones oficiales, sea cual fuere su pasaporte (de servicio no biométrico u ordinario).

- «b) para los hombres y mujeres de negocios y los representantes de organizaciones empresariales:
  - una invitación escrita procedente de la persona jurídica o empresa anfitrionas, o de una de sus oficinas o filiales, o bien de las autoridades nacionales o locales de los Estados miembros, o de un comité encargado de la organización de ferias, conferencias y simposios comerciales e industriales celebrados en el territorio de los Estados miembros;

- c) para los conductores que lleven a cabo servicios de transporte internacional de mercancías y pasajeros en el territorio de los Estados miembros en vehículos matriculados en Ucrania:
- una invitación escrita procedente de la asociación nacional de transportistas de Ucrania que presten servicios de transporte internacional por carretera, en la que se indiquen el objeto, la duración, el (los) destino(s) y la frecuencia de los viajes;»

Las autoridades competentes que prevean el transporte internacional por carretera y que sean responsables de que se indique el objeto, la duración, el (los) destino(s) y la frecuencia de los viajes de los conductores que lleven a cabo servicios de transporte internacional de mercancías y de pasajeros a los territorios de los Estados miembros en vehículos matriculados en Ucrania, son:

1. Association of International Road Carriers of Ukraine (AsMAP/«АсМАП»)

Dirección postal de la AsMAP:

11, Shorsa str.

Kyiv, 03150, Ucrania

Funcionarios habilitados para firmar las invitaciones:

Leonid Kostiuhenko — presidente de la AsMAP de Ucrania;

Dokil' Leonid — vicepresidente de la AsMAP de Ucrania;

Kuchynskiy Yurii — vicepresidente de la AsMAP de Ucrania.

2. Empresa estatal *Service on International Road Carriages* (ES «SIRC»)

Dirección postal de la ES «SIRC»:

57, av. Nauky

Kyiv, 03083, Ucrania

Tel. +38 445242101

Fax +38 445240070

Funcionarios habilitados para firmar las invitaciones:

Tkachenko Anatolij — director de la ES «SIRC»;

Neronov Oleksandr — primer director adjunto de la ES «SIRC».

3. Ukrainian Road Transport and Logistics Union

Dirección postal de la *Ukrainian Road Transport and Logistics Union*:

28, Predslavinska str.

Kyiv, 03150, Ucrania

Tel./Fax +38 445287130/+38 445287146/+38 445294440

Funcionarios habilitados para firmar las invitaciones:

Lypovskiy Vitalij — presidente de la Unión

4. All-Ukrainian Association of Automobile Carriers (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

Dirección postal de la AAAC:

139, Velyka Vasylkivska str.

Kyiv, 03150, Ucrania

Tel./Fax +38 445387505, +38 445292521

Funcionarios habilitados para firmar las invitaciones:

Reva Vitalii (Віталій Рева)-presidente de la AAAC

Glavatskyi Petro (Петро Главатський)-vicepresidente de la AAAC

correo electrónico: vaap@i.com.ua

5. *All-Ukrainian Association of Automobile Carriers (AAAC) Всеукраїнська асоціація автомобільних перевізників*

Dirección postal de la AAAC:

3, Rayisy Okipnoyi str.

Kyiv, 02002, Ucrania

Tel./Fax +38 445174431, +38 445164726

Funcionarios habilitados para firmar las invitaciones:

Vakulenko Volodymyr (Вакулєнко Володимир Михайлович)-vicepresidente de la AAAC

6. *Ukrainian State Enterprise «Ukrinteravtoservice» Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів «Укрінтеравтосервіс»*

Dirección postal de la empresa estatal *Ukrinteravtoservice*:

57, av. Nauky

Kyiv, 03083, Ucrania

Funcionarios habilitados para firmar las invitaciones:

Dobrohod Serhii (Доброход Сергій Олександрович) — director general de la empresa estatal *Ukrinteravtoservice* (Tel. +38 445240999; Móvil +38 504638932);

Kubalska Svitlana (Кубальська Світлана Сергіївна) — directora general adjunta de la empresa estatal *Ukrinteravtoservice* (Tel. +38 445240999; Móvil +38 505508262).

Habida cuenta de los problemas que plantea actualmente esta categoría de solicitantes de visado, el Comité Mixto supervisará de cerca la aplicación de esta disposición.

«d) para el personal de los vagones, vagones frigoríficos y locomotoras de trenes internacionales que tengan como destino el territorio de los Estados miembros:

— una invitación escrita de la sociedad de ferrocarriles competente de Ucrania en la que se indique el objeto, la duración y la frecuencia de los viajes;»

La autoridad competente en el ámbito del transporte ferroviario de Ucrania es la Administración estatal de transporte ferroviario de Ucrania (*Ukrzaliznytsia/Укрзалізниця*).

Dirección postal de *Ukrzaliznytsia*:

5-7 Tverskaya str.

Kyiv, 03680, Ucrania

Según el reparto de responsabilidades en la dirección de *Ukrzaliznytsia*, los funcionarios encargados de facilitar la información relativa al objeto, la duración y la frecuencia de los viajes del personal de los vagones, vagones frigoríficos y locomotoras de trenes internacionales que tengan como destino el territorio de los Estados miembros son:

Bolobolin Serhii (Болоболін Сергій Петрович) — primer director general de *Ukrzaliznytsia* (Tel. +38 444650010);

Serhiyenko Mykola (Сергієнко Микола &#x0406;ванович) — primer director general adjunto de *Ukrzaliznytsia* (Tel. +38 444650001);

Zhurakivskyy Vitaliy (Жураківський Віталій Олександрович) — primer director general adjunto de *Ukrzaliznytsia* (Tel. +38 444650041);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) — director general adjunto de *Ukrzaliznytsia* (Tel. +38 444650014);

Naumenko Petro (Науєнко Петро Петрович) — director general adjunto de *Ukrzaliznytsia* (Tel. +38 444650012);

Chekalov Pavlo (Чекалов Павло Леонтійович) — director general adjunto de *Ukrzaliznytsia* (Tel. +38 444650013);

Matviiv Igor — jefe de departamento de relaciones internacionales de *Ukrzaliznytsia* (Tel. +38 444650425).

«e) para los periodistas y el personal técnico que los acompañe por motivos profesionales:

- un certificado u otro documento expedido por una organización profesional o por el empleador del solicitante en el que se certifique que la persona en cuestión es un periodista cualificado, se acredite que el propósito del viaje es la realización de un trabajo periodístico o se demuestre que la persona es miembro del personal técnico que acompaña al periodista con fines profesionales;»

Esta categoría no incluye a los periodistas independientes.

Debe presentarse el certificado o documento que acredite que el solicitante es un periodista profesional y el documento original expedido por su empleador que indique que el objeto del viaje es la realización de un trabajo periodístico o acredite que la persona es miembro del personal técnico que acompaña al periodista con fines profesionales.

La organización profesional ucraniana que puede certificar que la persona en cuestión es un periodista cualificado es:

1. National Union of Journalists of Ukraine (NUJU) (Національна спілка журналістів України, НСЖУ).

NUJU expide a los empleados de medios de comunicación cualificados las tarjetas de periodistas profesionales nacionales y las tarjetas de prensa internacional siguiendo el modelo que exige la Federación Internacional de Periodistas.

Dirección postal de NUJU:

27-a Khreschatyk str.

Kyiv, 01001, Ucrania

Persona habilitada de la NUJU:

Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) — jefe de la NUJU

Tel./Fax +38 442342096; +38 442344960; +38 442345209

correo electrónico: [spilka@nsju.org](mailto:spilka@nsju.org); [admin@nsju.org](mailto:admin@nsju.org).

2. Independent MEDIA Union of Ukraine (IMUU) («Незалежна медіа-профспілка України»).

Dirección postal del IMUU:

Office 25,

27 — A, Khreshchatyk Str.,

Kyiv, 01001, Ucrania

Personas habilitadas:

Lukanov Yurii (Луканов Юрій Вадимович) — jefe de la IMUU

Vynnychuk Oksana (Оксана Винничук) — secretaria ejecutiva de la IMUU

Tel. +38 503565758

correo electrónico: [secretar@profspilka.org.ua](mailto:secretar@profspilka.org.ua)

«f) para las personas que participan en actividades científicas, culturales y artísticas, incluidos los programas de intercambio universitarios o de otro tipo:

- una invitación escrita de la organización anfitriona a participar en estas actividades;

g) para los estudiantes de los distintos ciclos, incluido el postgrado, y los profesores acompañantes que realicen viajes de estudios o con fines educativos en el marco de programas de intercambio o actividades extraescolares:

- una invitación escrita o un certificado de matriculación expedidos por la universidad, instituto o colegio anfitriones, o un carné de estudiante, o un certificado de los cursos a los que los visitantes piensan asistir;»

Solo podrá aceptarse un carné de estudiante como documento justificativo del objeto del viaje si ha sido expedido por la universidad, instituto o colegio en los que se van a cursar los estudios o la formación.

«h) para los participantes en eventos deportivos internacionales y las personas que los acompañan con fines profesionales:

— una invitación escrita procedente de la organización anfitriona: autoridades competentes, federaciones nacionales de deporte y comités olímpicos nacionales de los Estados miembros;»

La lista de los acompañantes en casos de actos deportivos internacionales se limitará a los que acompañen al deportista a título profesional: entrenadores, masajistas, patrocinadores, personal médico y presidente del club deportivo. No se considerarán acompañantes los seguidores).

«i) para los participantes en programas de intercambio oficiales organizados por las ciudades hermanadas y otros entes municipales:

— una petición escrita del alcalde o máxima autoridad de estas ciudades o de otros entes municipales;»

El alcalde/máxima autoridad de la ciudad u otra entidad municipal competente para la expedición de la invitación escrita es el alcalde o la máxima autoridad de la ciudad o el municipio en donde vaya a tener lugar el acto de hermanamiento. Esta categoría abarca únicamente los hermanamientos oficiales.

«j) para los parientes cercanos, como cónyuges, hijos (incluidos los adoptivos), padres (incluidos los tutores legales), abuelos y nietos, que visiten a nacionales ucranianos que residan legalmente en el territorio de los Estados miembros o a ciudadanos de la Unión Europea que residan en el territorio del Estado miembro del que son nacionales:

— una invitación escrita del anfitrión;»

Dicho párrafo regula la situación de los parientes cercanos ucranianos que viajen a los Estados miembros para visitar a nacionales ucranianos que residan legalmente en los Estados miembros o a ciudadanos de la Unión Europea que residan en el territorio del Estado miembro del que son nacionales.

La autenticidad de la firma de la persona de quien procede la invitación debe ser acreditada por la autoridad competente, de acuerdo con la legislación nacional del país de residencia.

También es necesario demostrar la residencia legal de la persona que cursa la invitación y el vínculo de parentesco; por ejemplo facilitando, junto con la invitación escrita del anfitrión, copias de documentos que expliquen su situación, como una fotocopia del permiso de residencia, y confirmen los vínculos de parentesco.

Dicha disposición se aplica también a los familiares del personal que trabaja en misiones diplomáticas y consulados que viajen para asistir a una reunión familiar de hasta noventa días al territorio de los Estados miembros, excepto en lo que se refiere a la necesidad de acreditar la residencia legal y los vínculos familiares.

En consonancia con la Declaración de la Unión Europea sobre facilidades para miembros de la familia, aneja al Acuerdo modificador, «Con el fin de facilitar los desplazamientos de un mayor número de personas con vínculos familiares (en particular, los hermanos, las hermanas y sus hijos) con ciudadanos de Ucrania que residan legalmente en el territorio de los Estados miembros o con ciudadanos de la Unión Europea que residan en el territorio del Estado miembro del que son nacionales, la Unión Europea insta a las oficinas consulares de los Estados miembros a aprovechar plenamente las posibilidades que ofrece el Código de visados para facilitar la expedición de visados a esta categoría de personas, en particular, la simplificación de los documentos justificativos exigidos a los solicitantes, la exención del pago de tasas de tramitación y, cuando proceda, la expedición de visados para entradas múltiples».

«k) para los parientes que se desplacen con ocasión de un entierro:

— un documento oficial en el que se certifique el fallecimiento y se confirme la relación de parentesco o de otro tipo entre el solicitante y el difunto;»

El Acuerdo no especifica qué autoridades nacionales deben expedir el referido documento oficial: el país en el que vaya a tener lugar el entierro o el país en el que reside la persona que desea asistir al mismo. Debe aceptarse que las autoridades competentes de ambos países pueden expedir este tipo de documento oficial.

Debe presentarse el referido documento oficial en el que se certifique el fallecimiento y se confirme la relación de parentesco o de otro tipo entre el solicitante y el difunto, por ejemplo, partida de nacimiento o acta de matrimonio.

«l) para las personas que deseen visitar un cementerio militar o civil:

— un documento oficial en el que se confirme la existencia y preservación de la tumba en cuestión, y que acredite la existencia de un parentesco u otro tipo de relación entre el solicitante y el difunto.»



El Acuerdo no especifica si el referido documento oficial debe ser expedido por las autoridades del país en el que se encuentra la tumba o las del país en el que reside la persona que desea visitar la tumba. Debe aceptarse que las autoridades competentes de ambos países pueden expedir este tipo de documento oficial.

Debe presentarse el referido documento oficial en el que se confirme la existencia y la preservación de la tumba así como la relación de parentesco o de otro tipo entre el solicitante y el difunto.

De conformidad con la Declaración de la Comunidad Europea aneja al Acuerdo, como regla general, los visados de corta duración para las personas que deseen visitar un cementerio militar o civil se expedirán por un período de hasta catorce días.

«m) para las personas que viajen por razones médicas y las personas que deban acompañarlas necesariamente:

- un documento oficial de la institución sanitaria en el que se confirme la necesidad del tratamiento médico en la misma, la necesidad de ser acompañadas y una acreditación de poseer los medios económicos suficientes para poder costearlo;»

Debe presentarse el documento de la institución sanitaria en el que se confirme la necesidad del tratamiento médico en dicha institución y una acreditación de poseer los medios económicos suficientes para poder costearlo, que debe confirmar asimismo la necesidad de ir acompañados.

«n) para los representantes de organizaciones de la sociedad civil que se desplacen para recibir formación o participar en seminarios y conferencias, por ejemplo en el marco de programas de intercambio:

- una petición escrita expedida por la organización anfitriona, una confirmación de que la persona está representando a la organización correspondiente y el certificado de inscripción de dicha organización en el registro pertinente, expedido por una autoridad estatal con arreglo a la legislación nacional;»

El documento que acredite la inscripción en Ucrania de una organización de la sociedad civil es una carta expedida por el Servicio de Registro estatal de Ucrania con la información del Registro de asociaciones públicas.

«o) para los miembros de profesiones liberales que participen en ferias, conferencias, simposios, seminarios internacionales o actos similares celebrados en el territorio de los Estados miembros;

- una invitación escrita de la organización anfitriona en la que se confirme la participación de la persona interesada en el acto correspondiente;

p) para los representantes de las comunidades religiosas;

- una invitación escrita de una comunidad religiosa reconocida en Ucrania, en la que se indique el objeto, la duración y la frecuencia de los desplazamientos;»

El documento que acredita el registro en Ucrania de una comunidad religiosa es un extracto del Registro estatal unificado de entidades jurídicas y empresarios particulares que indique que la entidad jurídica en cuestión es, por su forma organizativa y jurídica, una comunidad religiosa.

«q) para los participantes en programas oficiales de cooperación transfronteriza de la Unión Europea, por ejemplo en el marco del Instrumento Europeo de Vecindad y Asociación (IEVA):

- una solicitud escrita de la organización anfitriona.»

Importante: el Acuerdo no crea nuevas normas en materia de responsabilidad de las personas físicas o jurídicas que cursan las invitaciones escritas. En caso de falsedad en la expedición de las referidas invitaciones se aplicará el Derecho de la UE/nacional respectivo.

#### 2.2.2. Expedición de visados de entrada múltiple.

En los casos en que el solicitante de visado haya de viajar frecuente o regularmente al territorio de los Estados miembros, se expedirán visados de corta duración para múltiples estancias, siempre que la duración total de estas estancias no exceda de noventa días por período de ciento ochenta días.

El artículo 5, apartado 1, del Acuerdo establece lo siguiente:

«1. Las misiones diplomáticas y oficinas consulares de los Estados miembros expedirán visados de entrada múltiple, con un plazo de validez de cinco años, a las siguientes categorías de ciudadanos:

- a) los miembros de los gobiernos y parlamentos nacionales y regionales, de los tribunales constitucional y supremo, los fiscales nacionales y regionales y sus fiscales adjuntos, siempre que no estén exentos de la obligación de visado en virtud del presente Acuerdo, en el ejercicio de sus funciones;

- b) los miembros permanentes de delegaciones oficiales que, a raíz de una invitación oficial dirigida a Ucrania, participen regularmente en reuniones, consultas, negociaciones o programas de intercambio, así como en eventos celebrados por organizaciones intergubernamentales en el territorio de los Estados miembros;
- c) los cónyuges e hijos (incluidos los adoptivos) menores de 21 años o dependientes, así como los padres (incluidos los tutores legales) que visiten a ciudadanos de Ucrania que residen legalmente en el territorio de los Estados miembros o a ciudadanos de la Unión Europea que residen en el territorio del Estado miembro del que son nacionales;
- d) los hombres y mujeres de negocios y los representantes de empresas que viajen regularmente a los Estados miembros;
- e) los periodistas y el personal técnico que los acompañe por motivos profesionales.

No obstante lo dispuesto en el párrafo primero, cuando la necesidad o la intención de viajar frecuente o regularmente se limite manifiestamente a un período más corto, el plazo de validez del visado para entradas múltiples se limitará a dicho período, en particular cuando:

- en el caso de las personas mencionadas en la letra a), el mandato,
- en el caso de las personas mencionadas en la letra b), el período de duración de la condición de miembro permanente de la delegación oficial,
- en el caso de las personas mencionadas en la letra c), el período de validez de la autorización de residencia legal de los ciudadanos de Ucrania que residen legalmente en la Unión Europea,
- en el caso de las personas mencionadas en la letra d), el período de duración de la condición de representante de la organización empresarial o del contrato de trabajo,
- en el caso de las personas mencionadas en la letra e), el contrato de trabajo

tenga una duración inferior a cinco años.».

Para esas categorías de personas, teniendo en cuenta su situación profesional o la relación de parentesco con un ciudadano ucraniano que resida legalmente en el territorio de los Estados miembros o un ciudadano de la Unión Europea que resida en el territorio del Estado miembro del que es nacional, está justificado expedir, por regla general, un visado para entradas múltiples con una validez de cinco años. En la versión inicial del Acuerdo, la expresión «con un plazo de validez de hasta cinco años» dejaba libertad a los consulados para decidir sobre el período de validez del visado, estableciendo solo la duración máxima de validez. En virtud del Acuerdo modificador, esta facultad discrecional ha desaparecido al establecerse, con la nueva redacción «con un plazo de validez de cinco años», que, en caso de que el solicitante cumpla todos los requisitos del artículo 5, apartado 1, del Acuerdo, «las misiones diplomáticas y oficinas consulares de los Estados miembros expedirán visados de entrada múltiple, con un plazo de validez de hasta cinco años».

En el caso de las personas contempladas en el artículo 5, apartado 1, letra a), del Acuerdo, deberá confirmarse su situación profesional y la duración de su mandato.

Dicha disposición no se aplicará a las personas contempladas en el artículo 5, apartado 1, letra a), del Acuerdo, si están exentos de la obligación de visado en virtud del Acuerdo, es decir, si son titulares de un pasaporte diplomático o de un pasaporte de servicio biométrico.

En el caso de las personas contempladas en el artículo 5, apartado 1, letra b), del Acuerdo, deberá acreditarse su mandato de miembro permanente de la delegación y la necesidad de participar regularmente en reuniones, consultas, negociaciones o programas de intercambio.

En el caso de las personas contempladas en el artículo 5, apartado 1, letra c), del Acuerdo, deberá acreditarse la residencia legal del anfitrión (véase, más arriba, el punto II.2.2.1).

En el caso de las personas contempladas en el artículo 5, apartado 1, letras d) y e), del Acuerdo, deberá acreditarse su situación profesional y la duración de sus actividades.

El artículo 5, apartado 2, del Acuerdo establece lo siguiente:

«2. Las misiones diplomáticas y oficinas consulares de los Estados miembros expedirán visados de entrada múltiple, con un plazo de validez de un año, a las siguientes categorías de ciudadanos, siempre que durante el año anterior a la solicitud estas personas hayan obtenido al menos un visado, y lo hayan utilizado de acuerdo con la legislación sobre entrada y estancia en el territorio del Estado anfitrión:

- a) los conductores que presten en vehículos matriculados en Ucrania servicios de transporte internacional de mercancías y pasajeros que tengan como destino el territorio de los Estados miembros;

- b) el personal de los vagones, vagones frigoríficos y locomotoras de los trenes internacionales que tengan como destino el territorio de los Estados miembros;
- c) las personas que participen en actividades científicas, culturales y artísticas, incluidos los programas de intercambio universitarios o de otro tipo, y que viajen regularmente a los Estados miembros;
- d) los participantes en eventos deportivos internacionales y las personas que los acompañan con fines profesionales;
- e) las personas que participen en programas oficiales de intercambio organizados por las ciudades hermanadas y otros entes municipales;
- f) los representantes de organizaciones de la sociedad civil que viajen frecuentemente a los Estados miembros para recibir formación o participar en seminarios y conferencias, por ejemplo en el marco de programas de intercambio;
- g) los participantes en programas oficiales de cooperación transfronteriza de la Unión Europea, por ejemplo en el marco del Instrumento Europeo de Vecindad y Asociación (IEVA);
- h) los estudiantes y estudiantes de posgrado que realicen periódicamente viajes de estudios o con fines educativos, incluso en el marco de programas de intercambio;
- i) los representantes de comunidades religiosas;
- j) los miembros de profesiones liberales que participen en ferias, conferencias, simposios, seminarios internacionales o actos similares celebrados en el territorio de los Estados miembros;
- k) personas que deban viajar frecuentemente por razones médicas y las personas que deban acompañarlas.

No obstante lo dispuesto en el primer párrafo, cuando la necesidad o la intención de viajar frecuente o regularmente se limite manifiestamente a un período más corto, el plazo de validez del visado para entradas múltiples se limitará a dicho período.».

En la versión inicial del Acuerdo, la expresión «con un plazo de validez de hasta un año» dejaba a los consulados un margen de apreciación a la hora de determinar el período de validez del visado, estableciendo solo la duración máxima de validez. En virtud del Acuerdo modificador, esta facultad discrecional ha desaparecido al establecerse, con la nueva redacción «con un plazo de validez de un año», que, en caso de que el solicitante cumpla todos los requisitos del artículo 5, apartado 2, del Acuerdo, «las misiones diplomáticas y oficinas consulares de los Estados miembros expedirán visados de entrada múltiple, con un plazo de validez de un año». Téngase presente que se expedirán visados para entradas múltiples con una validez de un año a las referidas categorías si durante el año (doce meses) anterior, el solicitante de visado ha obtenido al menos un visado Schengen y ha hecho uso de él de conformidad con la legislación sobre entrada y estancia del Estado o los Estados visitados (por ejemplo, la persona no ha sobrepasado la duración de estancia autorizada) y si hay razones para solicitar un visado para entradas múltiple. El visado Schengen obtenido durante el año anterior puede haber sido expedido por otro Estado Schengen distinto a aquel en que el solicitante solicitó el nuevo visado. En los casos en que no está justificada la expedición de un visado de un año de validez (por ejemplo, cuando la duración del programa de intercambio sea de menos de un año o la persona no necesite viajar frecuente o regularmente durante todo un año), el período de validez del visado será inferior a un año, siempre que se cumplan los demás requisitos para la expedición del visado.

El artículo 5, apartados 3 y 4, del Acuerdo establece lo siguiente:

«3. Las misiones diplomáticas y oficinas consulares de los Estados miembros expedirán visados de entrada múltiple, con un plazo de validez de un mínimo de dos años y un máximo de cinco años, a las categorías de personas citadas en el apartado 2 del presente artículo, siempre que durante los dos años anteriores a la solicitud estas personas hayan utilizado su visado de entrada múltiple de una duración de un año de acuerdo con la legislación sobre la entrada y estancia en el territorio del Estado anfitrión, a menos que la necesidad o la intención de viajar frecuente o regularmente se haya manifiestamente limitado a un período más corto, en cuyo caso el plazo de validez del visado de entrada múltiple se limitará a dicho período.

4. La duración total de la estancia de las personas mencionadas en los apartados 1 a 3 del presente artículo en el territorio de los Estados miembros no podrá exceder de noventa días por período de ciento ochenta días.»

Se expedirán visados para entradas múltiples con una validez de entre dos y cinco años a las categorías mencionadas en el artículo 5, apartado 2, del Acuerdo, siempre que durante los dos años anteriores hayan hecho uso de los visados Schengen para entradas múltiples de un año de validez de conformidad con la legislación sobre entrada y estancia en el territorio o los territorios del Estado o Estados visitados y que la necesidad de viajar frecuente o regularmente no se limite manifiestamente a un período más breve. Ha de tenerse en cuenta que solo se expedirá un visado con una validez de dos a cinco años si se ha expedido al solicitante de visado dos visados con una validez de un año —como mínimo— durante los dos años anteriores, y si ha hecho uso de estos visados de conformidad con la legislación sobre entrada y estancia en el territorio o territorios del Estado o los Estados visitados. Las misiones diplomáticas y las oficinas consulares de los Estados miembros decidirán, sobre la base de la evaluación de cada solicitud de visado, el plazo de validez de dichos visados, es decir, de dos a cinco años.

En cuanto a la definición de los criterios que figuran en el artículo 5, apartado 2, del Acuerdo: «siempre que [...] tengan razones para solicitar un visado de entrada múltiple», y en el artículo 5, apartado 3, del Acuerdo: «siempre que [...] sus razones para solicitar un visado de entrada múltiple sigan siendo válidas», se aplicarán los criterios que figuran en el artículo 24, apartado 2, letra a), del Código de visados para la expedición de esos tipos de visados, es decir, que la persona en cuestión necesite viajar frecuentemente a uno o varios Estados miembros, por ejemplo por negocios.

No existe obligación alguna de expedir un visado para entradas múltiples si el solicitante no hizo uso de un visado anterior. No obstante, dicho visado puede expedirse si la no utilización del visado anterior se debe a circunstancias independientes de la voluntad del solicitante; por ejemplo, una larga ausencia de su puesto de trabajo de un conductor de camiones por causa de enfermedad.

Véase el punto II.2.2.1. por lo que respecta a los documentos que justifican el objeto del viaje para la expedición de visados de entradas múltiples a las categorías mencionadas en el artículo 5 del Acuerdo.

#### 2.2.3. Titulares de pasaportes diplomáticos y de servicio

El artículo 10 del Acuerdo dispone lo siguiente:

- «1. Los ciudadanos de Ucrania que sean titulares de pasaportes diplomáticos válidos pueden entrar, salir y transitar por los territorios de los Estados miembros sin visado.
2. Los ciudadanos de Ucrania que sean titulares de pasaportes de servicio biométricos válidos podrán entrar, salir y transitar por los territorios de los Estados miembros sin visado.
3. Las personas citadas en los apartados 1 y 2 del presente artículo podrán residir en el territorio de los Estados miembros por un período de tiempo que no deberá exceder de 90 días por período de 180 días.»

Los acuerdos o compromisos bilaterales que prevean la exención de visado para los titulares de pasaportes de servicio no biométricos seguirán aplicándose, salvo denuncia notificada o suspendida (véase I.1.6).

El nombramiento de diplomáticos destacados en los Estados miembros no está regulado por el Acuerdo. Se aplica el procedimiento habitual de acreditación.

### III. ESTADÍSTICA

Con el fin de permitir al Comité Mixto supervisar de forma efectiva el Acuerdo, las misiones diplomáticas y las oficinas consulares de los Estados miembros deben facilitar estadísticas a la Comisión cada seis meses, en relación, en particular, de ser posible, y especificando por mes:

- los tipos de visados expedidos a las distintas categorías de personas cubiertas por el Acuerdo;
- el número de denegaciones de visado para las diferentes categorías de personas cubiertas por el Acuerdo;
- los porcentajes de solicitantes convocados a una entrevista personal por categorías de personas;
- los visados de entrada múltiple de cinco años de validez expedidos a nacionales ucranianos (por país).
- los porcentajes de visados expedidos gratuitamente a las diferentes categorías de personas cubiertas por el Acuerdo.

**DECISIÓN (PESC) 2015/439 DEL CONSEJO****de 16 de marzo de 2015****por la que se prorroga el mandato del Representante Especial de la Unión Europea para el Sahel**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, su artículo 33 y su artículo 31, apartado 2,

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

Considerando lo siguiente:

- (1) El 18 de marzo de 2013, el Consejo adoptó la Decisión 2013/133/PESC <sup>(1)</sup> por la que se nombra a D. Michel Dominique REVEYRAND — DE MENTHON Representante Especial de la Unión Europea (REUE) para el Sahel. El mandato del REUE se prorrogó mediante Decisión 2014/130/PESC del Consejo <sup>(2)</sup> y expira el 28 de febrero de 2015.
- (2) El mandato del REUE debe prorrogarse por un nuevo período de ocho meses.
- (3) El REUE ejecutará su mandato en el contexto de una situación que puede deteriorarse y que podría perjudicar a los objetivos de la acción exterior de la Unión establecidos en el artículo 21 del Tratado.

HA ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1***Representante Especial de la Unión Europea**

1. Queda prorrogado hasta el 31 de octubre de 2015 el mandato de D. Michel Dominique REVEYRAND — DE MENTHON como REUE para el Sahel. El mandato del REUE podrá concluir antes si así lo decidiera el Consejo, a propuesta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (AR).
2. A efectos del mandato del REUE, se define el Sahel como la zona que constituye el centro principal de la Estrategia de la UE para la seguridad y el desarrollo en el Sahel («la Estrategia»), en concreto Burkina Faso, Chad, Mali, Mauritania y Níger. Para las cuestiones con implicaciones regionales más amplias, el REUE establecerá contactos con otros países vecinos y entidades regionales o internacionales más allá del Sahel, y también África occidental y el Golfo de Guinea, según corresponda.
3. Dada la necesidad de un planteamiento regional para los desafíos interconectados a que se enfrenta la región, el REUE para el Sahel desempeñará su mandato en estrecha consulta con otros REUE pertinentes, incluido el REUE para la región del Mediterráneo Meridional, el REUE para los Derechos Humanos y el REUE para la Unión Africana.

*Artículo 2***Objetivos de actuación**

1. El mandato del REUE se basará en el objetivo de actuación de la Unión en relación con el Sahel de contribuir activamente a los esfuerzos regionales e internacionales por conseguir una paz duradera, la seguridad y el desarrollo en la región. El REUE procurará, además, mejorar la calidad, la intensidad y los efectos de la acción multifacética de la Unión en el Sahel.
2. El REUE contribuirá al desarrollo y la aplicación del enfoque de la Unión, que abarcará todos los aspectos de la acción de la Unión, particularmente en los ámbitos político, de seguridad y de desarrollo, incluida la Estrategia, y a coordinar todos los instrumentos pertinentes para las acciones de la Unión.
3. Se otorgará la prioridad inicial a Mali y a su estabilización a largo plazo así como a las dimensiones regionales de ese conflicto.

<sup>(1)</sup> Decisión 2013/133/PESC del Consejo, de 18 de marzo de 2013, por la que se nombra al Representante Especial de la Unión Europea para el Sahel (DO L 75 de 19.3.2013, p. 29).

<sup>(2)</sup> Decisión 2014/130/PESC del Consejo, de 10 de marzo de 2014, por la que se prorroga el mandato del Representante Especial de la Unión Europea para el Sahel (DO L 71 de 12.3.2014, p. 14).

4. Respecto de Mali, los objetivos de actuación de la Unión serán promover, mediante el uso coordinado y eficaz de todos sus instrumentos, el retorno de Mali y de su pueblo a una senda de paz, reconciliación, seguridad y desarrollo. Se prestará la debida atención a Burkina Faso y Níger, en particular en la perspectiva de las elecciones que han de celebrarse en esos países.

### Artículo 3

#### Mandato

1. A fin de alcanzar los objetivos de actuación en relación con el Sahel, el mandato del REUE consistirá en:
  - a) contribuir activamente a la aplicación, la coordinación y el desarrollo sucesivo del enfoque global de la Unión respecto de la crisis regional, sobre la base de su Estrategia, a fin de mejorar la coherencia y la eficacia generales de las actividades de la Unión en el Sahel, en particular en Mali;
  - b) establecer contactos con todos los actores de la región, gobiernos, autoridades regionales y organizaciones regionales e internacionales, la sociedad civil y la diáspora, a fin de promover los objetivos de la Unión y contribuir a una mejor comprensión del papel de la Unión en el Sahel;
  - c) representar a la Unión en los foros regionales e internacionales pertinentes, incluido el Grupo de Apoyo y de Seguimiento de la situación de Mali, y dar visibilidad al apoyo de la Unión a la gestión de crisis y la prevención de conflictos, incluida la misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas armadas de Mali (EUTM Mali) y a la Misión PCSD de la Unión Europea en Níger (EUCAP Sahel Níger);
  - d) mantener una estrecha cooperación con las Naciones Unidas (ONU), en particular con el Representante Especial del Secretario General para África Occidental, y el Representante Especial del Secretario General para Mali, la Unión Africana (UA), en particular el Alto Representante de la UA para Mali y el Sahel, la Comunidad Económica de los Estados del África Occidental (CEDEAO) y otros actores nacionales, regionales e internacionales destacados, incluidos otros Enviados Especiales para el Sahel, así como con los organismos pertinentes de la zona del Magreb;
  - e) seguir de cerca la dimensión regional y transfronteriza de la crisis, con inclusión del terrorismo, la delincuencia organizada, el contrabando de armas, el tráfico de seres humanos, el tráfico de drogas, los flujos de refugiados y migratorios y los flujos financieros conexos, y contribuir, en estrecha cooperación con el Coordinador de la lucha contra el terrorismo de la UE, al desarrollo de la Estrategia de la UE de Lucha contra el Terrorismo;
  - f) mantener periódicamente contactos políticos de alto nivel con los países de la región afectados por el terrorismo y la delincuencia internacional a fin de garantizar un enfoque coherente y global y asegurar un papel determinante de la Unión en los esfuerzos internacionales por combatir el terrorismo y la delincuencia internacional. Esto incluye el apoyo activo de la Unión al desarrollo de capacidades regionales en el ámbito de la seguridad, y garantizar que se aborden adecuadamente las causas primeras del terrorismo y la delincuencia internacional en el Sahel;
  - g) hacer un estrecho seguimiento de las consecuencias políticas y de seguridad que tienen las crisis humanitarias en la región;
  - h) con respecto a Mali, contribuir a los esfuerzos regionales e internacionales para facilitar la resolución de la crisis de Mali, en particular un restablecimiento total de la normalidad constitucional y la gobernanza en todo el territorio y un diálogo nacional que sea creíble e integrador y que lleve a un asentamiento político sostenible;
  - i) fomentar el desarrollo institucional, la reforma del sector de la seguridad y la construcción de la paz y la reconciliación a largo plazo en Mali;
  - j) contribuir a la aplicación de la política de derechos humanos de la Unión en la región, en cooperación con el REUE para los Derechos Humanos, incluidas las Directrices de la UE sobre derechos humanos, incluidas las Directrices de la UE sobre los niños y los conflictos armados, y sobre la violencia contra las mujeres y las niñas y la lucha contra todas las formas de discriminación contra ellas, y de las políticas de la Unión sobre la mujer, la paz y la seguridad, lo que incluye hacer un seguimiento e informar de la evolución, así como formular recomendaciones a este respecto, y mantener contactos periódicos con las autoridades relevantes de Mali y de la región, la Oficina del Fiscal de la Corte Penal Internacional, la Oficina del Alto Comisionado para los Derechos Humanos y los defensores y observadores de los derechos humanos de la región;
  - k) hacer un seguimiento e informar sobre la observancia de las resoluciones pertinentes del Consejo de Seguridad de la ONU, en particular las Resoluciones 2056 (2012), 2071 (2012), 2085 (2012) y 2100 (2013).
2. A efectos del cumplimiento de su mandato, corresponderá al REUE, entre otras actividades:
  - a) asesorar e informar sobre la formulación de las posiciones de la Unión en los foros regionales e internacionales, según proceda, a fin de promover y reforzar de manera anticipatoria el enfoque global de la Unión respecto de la crisis en el Sahel;
  - b) tener una visión de conjunto de todas las actividades de la Unión y cooperar estrechamente con las delegaciones de la Unión correspondientes.

*Artículo 4***Ejecución del mandato**

1. El REUE será responsable de la ejecución del mandato bajo la autoridad de la AR.
2. El Comité Político y de Seguridad (CPS) mantendrá una relación privilegiada con el REUE y será su principal punto de contacto con el Consejo. El CPS proporcionará al REUE orientaciones estratégicas y dirección política en el marco del mandato, sin perjuicio de las competencias de la AR.
3. El REUE actuará en estrecha coordinación con el Servicio Europeo de Acción Exterior (SEAE) y con sus departamentos competentes, en particular con el Coordinador para la región del Sahel.

*Artículo 5***Financiación**

1. El importe de referencia financiera destinado a cubrir los gastos relacionados con el mandato del REUE durante el período comprendido entre el 1 de marzo de 2015 y el 31 de octubre de 2015 será de 900 000 EUR.
2. Los gastos se gestionarán con arreglo a los procedimientos y normas aplicables al presupuesto general de la Unión.
3. La gestión del gasto se regirá por un contrato entre el REUE y la Comisión. El REUE rendirá cuentas a la Comisión de todos los gastos.

*Artículo 6***Constitución y composición del equipo**

1. Dentro de los límites establecidos en su mandato y de los medios financieros correspondientes puestos a su disposición, el REUE será responsable de constituir su equipo. El equipo incluirá personal especializado en las cuestiones políticas específicas que prevea el mandato. El REUE informará sin demora al Consejo y a la Comisión de la composición del equipo.
2. Los Estados miembros, las instituciones de la Unión y el SEAE podrán proponer el envío de personal en comisión de servicio para que trabaje con el REUE. La retribución de este personal enviado en comisión de servicio ante el REUE será sufragada por el Estado miembro de que se trate, la institución de la Unión de que se trate o el SEAE. También podrán asignarse al REUE expertos enviados por los Estados miembros en comisión de servicio a las instituciones de la Unión o el SEAE. El personal internacional contratado tendrá la nacionalidad de un Estado miembro.
3. Todo el personal en comisión de servicio seguirá dependiendo administrativamente del Estado miembro, de la institución de la Unión o del SEAE, y desempeñará sus funciones y actuará en interés del mandato del REUE.
4. El personal del REUE será destinado a los departamentos correspondientes del SEAE o las delegaciones de la Unión a fin de garantizar la coherencia y compatibilidad de sus actividades respectivas.

*Artículo 7***Privilegios e inmunidades del REUE y de su personal**

Los privilegios, inmunidades y otras garantías necesarias para la realización y buen funcionamiento de la misión del REUE y para los miembros de su personal se acordarán con los países anfitriones, según proceda. Los Estados miembros y el SEAE concederán todo el apoyo necesario a tal fin.

*Artículo 8***Seguridad de la información clasificada de la UE**

El REUE y los miembros de su equipo respetarán los principios de seguridad y normas mínimas establecidos en la Decisión 2013/488/UE del Consejo <sup>(1)</sup>.

<sup>(1)</sup> Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).

*Artículo 9***Acceso a la información y apoyo logístico**

1. Los Estados miembros, la Comisión, el SEAE y la Secretaría General del Consejo velarán por que el REUE tenga acceso a cualquier información pertinente.
2. Las delegaciones de la Unión y/o los Estados miembros, según proceda, proporcionarán apoyo logístico en la región.

*Artículo 10***Seguridad**

De conformidad con la política de la Unión sobre la seguridad del personal enviado fuera de la Unión con funciones operativas en virtud del título V del Tratado, el REUE tomará todas las medidas razonables, de conformidad con su mandato y a tenor de la situación de la seguridad en la zona geográfica de la que sea responsable, para garantizar la seguridad de todo el personal que se halle bajo su autoridad directa, en particular:

- a) estableciendo un plan de seguridad específico, basado en las orientaciones del SEAE, que comprenda medidas de seguridad físicas, organizativas y de procedimiento específicas, por el que se rijan la gestión de los desplazamientos seguros del personal a la zona geográfica y dentro de ella y la gestión de los incidentes de seguridad, así como un plan de contingencia y de evacuación de la misión;
- b) garantizando que todo el personal desplegado fuera de la Unión esté cubierto por un seguro de alto riesgo que corresponda a las condiciones de la zona geográfica;
- c) garantizando que todos los miembros del equipo que hayan de desempeñar sus funciones fuera de la Unión, incluido el personal local contratado, hayan recibido antes de llegar a la zona de la misión o inmediatamente después de hacerlo, la formación adecuada en materia de seguridad acorde con el grado de riesgo asignado a esa zona;
- d) garantizando la aplicación de todas las recomendaciones convenidas que se deriven de las evaluaciones periódicas de seguridad y facilitando informes escritos al Consejo, a la AR y a la Comisión sobre dicha aplicación y sobre otras cuestiones relativas a la seguridad, en el marco del informe de situación y del informe de ejecución del mandato.

*Artículo 11***Informes**

1. El REUE presentará informes a la AR y al CPS con carácter periódico. En caso necesario, el REUE también informará a los grupos de trabajo del Consejo. Los informes periódicos se transmitirán a través de la red COREU. El REUE podrá presentar informes al Consejo de Asuntos Exteriores. En virtud del artículo 36 del Tratado, el REUE podrá estar asociado a la información al Parlamento Europeo.
2. El REUE informará sobre la manera más adecuada de realizar las iniciativas de la Unión, tales como la contribución de la Unión a reformas, incluidos los aspectos políticos de los proyectos de desarrollo de la Unión pertinentes, en coordinación con las delegaciones de la Unión en la región.

*Artículo 12***Coordinación con otros actores de la Unión**

1. En el marco de la Estrategia, el REUE contribuirá a la unidad, la coherencia y la eficacia de la acción política y diplomática de la Unión, así como a garantizar que todos los instrumentos de la Unión y acciones de los Estados miembros se desarrollen de manera coherente a fin de lograr los objetivos de actuación de la Unión.
2. Las actividades del REUE se coordinarán con las de las delegaciones de la Unión y las de la Comisión, así como con las de otros REUE que actúen en la región. El REUE ofrecerá periódicamente sesiones informativas dirigidas a las misiones de los Estados miembros y a las delegaciones de la Unión presentes en la región.
3. Sobre el terreno, se mantendrá una relación estrecha con los jefes de las delegaciones de la Unión y los jefes de misión de los Estados miembros. El REUE, en estrecha cooperación con las delegaciones de la Unión, proporcionará orientación política a los Jefes de la misión EUCAP Sahel Níger, de la misión EUCAP Sahel Mali y al Comandante de la misión EUTM Mali. El REUE, el Comandante de EUTM Mali y el Comandante de la operación civil de EUCAP Sahel Níger y EUCAP Sahel Mali se consultarán mutuamente según sea necesario.



*Artículo 13***Revisión**

La aplicación de la presente Decisión y su coherencia con las demás contribuciones de la Unión a la región se revisará con carácter periódico. El REUE presentará al Consejo, a la AR y a la Comisión un informe global sobre la ejecución de su mandato a más tardar a finales de agosto de 2015.

*Artículo 14***Entrada en vigor**

La presente Decisión entrará en vigor el día de su adopción.

Será aplicable desde el 1 de marzo de 2015.

Hecho en Bruselas, el 16 de marzo de 2015.

*Por el Consejo*  
*La Presidenta*  
F. MOGHERINI

---

**DECISIÓN (PESC) 2015/440 DEL CONSEJO****de 16 de marzo de 2015****por la que se prorroga el mandato del Representante Especial de la Unión Europea para el Cuerno de África**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, su artículo 31, apartado 2, y su artículo 33,

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

Considerando lo siguiente:

- (1) El 8 de diciembre de 2011, el Consejo adoptó la Decisión 2011/819/PESC <sup>(1)</sup> por la que se nombraba a D. Alexander RONDOS Representante Especial de la Unión Europea (REUE) para el Cuerno de África. El mandato del REUE expira el 28 de febrero de 2015.
- (2) El mandato del REUE debe, pues, prorrogarse hasta el 31 de octubre de 2015.
- (3) El REUE ejecutará su mandato en el contexto de una situación que puede deteriorarse y podría dificultar el logro de los objetivos de la acción exterior de la Unión enunciados en el artículo 21 del Tratado.

HA ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1***Representante Especial de la Unión Europea**

El mandato de D. Alexander RONDOS en tanto que Representante Especial de la Unión Europea (REUE) para el Cuerno de África queda prorrogado hasta el 31 de octubre de 2015. El Consejo podrá decidir que el mandato del REUE concluya antes, en base al asesoramiento del Comité Político y de Seguridad (CPS) y a propuesta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad (AR).

A efectos del mandato del REUE, se define el Cuerno de África como la región integrada por: la República de Yibuti, el Estado de Eritrea, la República Federal Democrática de Etiopía, la República de Kenia, la República Federal de Somalia, la República de Sudán, la República de Sudán del Sur y la República de Uganda. Para cuestiones con implicaciones regionales más amplias, el REUE tomará contacto, si es necesario, con países y entidades regionales exteriores al Cuerno de África.

*Artículo 2***Objetivos políticos**

1. El mandato del REUE se basará en los objetivos políticos de la Unión con respecto al Cuerno de África tal como se establecieron en el marco estratégico adoptado el 14 de noviembre de 2011 y en las conclusiones del Consejo correspondientes, a fin de, en particular, contribuir activamente a los esfuerzos regionales e internacionales por lograr una coexistencia pacífica y una paz, seguridad y desarrollo duraderos entre los países de la región y en cada uno de ellos. El REUE procurará, además, mejorar la calidad, la intensidad, los efectos y la visibilidad de la acción polifacética de la Unión en el Cuerno de África.
2. Dichos objetivos políticos son, entre otros:
  - a) la continuación de la estabilización de Somalia, en particular abordándola desde una dimensión regional;
  - b) la coexistencia pacífica de Sudán y Sudán del Sur como dos Estados viables y prósperos con estructuras políticas sólidas y responsables;
  - c) la resolución de los conflictos actuales evitando posibles conflictos entre los países de la región o dentro de ellos;
  - d) el apoyo a la cooperación regional en materia de política, seguridad y economía.

<sup>(1)</sup> Decisión 2011/819/PESC del Consejo, de 8 de diciembre de 2011, por la que se nombra al Representante Especial de la Unión Europea para el Cuerno de África (DO L 327 de 9.12.2011, p. 62).

*Artículo 3***Mandato**

1. Para alcanzar los objetivos políticos de la Unión en relación con el Cuerno de África, el mandato del REUE consistirá en:
  - a) actuar junto a todas las partes pertinentes de la región, gobiernos, autoridades regionales, organizaciones internacionales y regionales, sociedad civil y diásporas a fin de perseguir los objetivos de la Unión y contribuir a una mejor comprensión del papel de la Unión en la región;
  - b) representar, si procede, a la Unión en los foros internacionales pertinentes y garantizar la visibilidad del apoyo de la Unión a la gestión de crisis y a la resolución y prevención de conflictos;
  - c) alentar y apoyar una cooperación efectiva en política y seguridad y la integración económica efectiva en la región mediante la asociación de la Unión con la Unión Africana (UA) y con organizaciones regionales, en particular la Autoridad Intergubernamental para el Desarrollo (IGAD);
  - d) seguir los acontecimientos políticos de la región y contribuir al desarrollo de la política de la Unión hacia la región, en particular en relación con Somalia, Sudán, Sudán del Sur, el problema de la frontera entre Etiopía y Eritrea y la aplicación del Acuerdo de Argel, la Iniciativa de la Cuenca del Nilo y otras preocupaciones regionales que repercuten en la seguridad, la estabilidad y la prosperidad;
  - e) en lo que respecta a Somalia, y en estrecha coordinación con el Enviado Especial de la UE para Somalia y los socios regionales e internacionales pertinentes, incluidos el Representante Especial del Secretario General de las Naciones Unidas (ONU) para Somalia y la Unión Africana, contribuir activamente a las acciones e iniciativas que conduzcan a una mayor estabilización y unos acuerdos posteriores a la transición para Somalia, insistiendo en la promoción de un enfoque internacional coordinado y coherente para Somalia, el establecimiento de buenas relaciones de vecindad y el apoyo al desarrollo del sector de la seguridad en Somalia, contribuyendo también, a través de la misión militar de la Unión Europea, a la formación de las fuerzas de seguridad somalíes (EUTM Somalia), a la fuerza naval dirigida por la Unión Europea (EUNAVFOR Atalanta), a la Misión de la Unión Europea de desarrollo de las capacidades marítimas regionales en el Cuerno de África (EUCAP NESTOR), y al apoyo permanente de la Unión a la Misión de la Unión Africana en Somalia (AMISOM), en estrecha colaboración con los Estados miembros;
  - f) en cuanto a Sudán y Sudán del Sur, y en estrecha colaboración con los respectivos Jefes de delegación de la Unión, contribuir a la coherencia y la eficacia de la política de la Unión respecto a Sudán y Sudán del Sur y apoyar su coexistencia pacífica, en particular mediante la aplicación de los Acuerdos de Addis y la resolución de las cuestiones aún pendientes tras el Acuerdo de paz global, incluidas Abyei, las soluciones políticas a los conflictos en marcha, particularmente en Darfur, Kordofán del Sur y Nilo Azul, el desarrollo institucional en Sudán del Sur y la reconciliación nacional. A este respecto, el REUE contribuirá a un enfoque internacional coherente en estrecha cooperación con la UA y especialmente con el Grupo de Alto Nivel de la UA encargado de la aplicación de las recomendaciones para Sudán (AUHIP), la ONU y otras partes interesadas clave a escala regional e internacional;
  - g) efectuar un estrecho seguimiento de los retos transfronterizos que afectan al Cuerno de África, incluidos el terrorismo, la radicalización, la seguridad marítima y la piratería, la delincuencia organizada, el contrabando de armas, los flujos de refugiados y migrantes, y las consecuencias políticas y de seguridad de las crisis humanitarias;
  - h) promover el acceso a la ayuda humanitaria en toda la región;
  - i) contribuir a la aplicación de la Decisión 2011/168/PESC del Consejo <sup>(1)</sup>, y de la política de la Unión relativa a los derechos humanos en colaboración con el REUE para los Derechos Humanos, incluidas las Directrices de la UE sobre derechos humanos, en particular las Directrices de la UE sobre los niños y los conflictos armados, así como las Directrices de la UE sobre la violencia contra las mujeres y las niñas y la lucha contra todas las formas de discriminación contra ellas, y la política de la Unión respecto a la Resolución del Consejo de Seguridad de la ONU 1325 (2000), entre otros medios a través del seguimiento y la elaboración de informes sobre la evolución de la situación, así como la formulación de recomendaciones al respecto.
2. A efectos del cumplimiento de su mandato, el REUE deberá, entre otras cosas:
  - a) asesorar e informar, si procede, sobre la definición de las posiciones de la Unión en los foros internacionales, a fin de fomentar proactivamente el planteamiento político global de la Unión para el Cuerno de África;
  - b) mantener una visión general de todas las actividades de la Unión.

<sup>(1)</sup> Decisión 2011/168/PESC del Consejo, de 21 de marzo de 2011, relativa a la Corte Penal Internacional y por la que se deroga la Posición Común 2003/444/PESC (DO L 76 de 22.3.2011, p. 56).

*Artículo 4***Ejecución del mandato**

1. El REUE será responsable de la ejecución del mandato bajo la autoridad de la AR.
2. El CPS mantendrá una relación privilegiada con el REUE y será el principal punto de contacto con el Consejo. El CPS proporcionará al REUE orientaciones estratégicas y dirección política en el marco del mandato, sin perjuicio de las competencias de la AR.
3. El REUE trabajará en estrecha coordinación con el Servicio Europeo de Acción Exterior (SEAE) y con sus departamentos competentes, las delegaciones de la Unión en la región y la Comisión.

*Artículo 5***Financiación**

1. El importe de referencia financiera previsto para cubrir los gastos relacionados con el mandato del REUE del 1 de marzo de 2015 al 31 de octubre de 2015 será de 1 770 000 EUR.
2. Los gastos se gestionarán con arreglo a los procedimientos y normas aplicables al presupuesto general de la Unión.
3. La gestión del gasto se regirá por un contrato entre el REUE y la Comisión. El REUE rendirá cuentas a la Comisión de todos los gastos.

*Artículo 6***Constitución y composición del equipo**

1. Dentro de los límites establecidos en su mandato y de los recursos financieros correspondientes que se hayan puesto a su disposición, el REUE será responsable de constituir su equipo. El equipo incluirá personal especializado en las cuestiones políticas y de seguridad específicas que prevea el mandato. El REUE mantendrá informados con puntualidad y de manera periódica al Consejo y a la Comisión de la composición de su equipo.
2. Los Estados miembros, las instituciones de la Unión y el SEAE podrán proponer el envío de personal en comisión de servicios para que trabaje con el REUE. El salario de ese personal enviado en comisión de servicios será sufragado por quien otorgue la comisión de servicios, ya sea el Estado miembro, la institución de la Unión interesada o el SEAE. Los Estados miembros también podrán asignar al REUE expertos enviados en comisión de servicios a las instituciones de la Unión o al SEAE. El personal internacional contratado deberá tener la nacionalidad de un Estado miembro.
3. Todo el personal en comisión de servicios seguirá dependiendo administrativamente del Estado miembro o de la institución de la Unión que lo haya enviado, o del SEAE, y desempeñará sus funciones y actuará en interés del mandato del REUE.
4. El personal del REUE compartirá ubicación con los departamentos pertinentes del SEAE o las delegaciones de la Unión con el fin de contribuir a la coherencia y correlación de sus respectivas actividades.

*Artículo 7***Privilegios e inmunidades del REUE y del personal del REUE**

Los privilegios, inmunidades y otras garantías necesarias para la realización y buen funcionamiento de la misión del REUE y de los miembros del personal del REUE se acordarán con los países anfitriones, según proceda. Los Estados miembros y el SEAE concederán todo el apoyo necesario a tal fin.

*Artículo 8***Seguridad de la información clasificada de la UE**

El REUE y los miembros de su equipo respetarán los principios de seguridad y las normas mínimas establecidos en la Decisión 2013/488/UE del Consejo <sup>(1)</sup>.

<sup>(1)</sup> Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).

*Artículo 9***Acceso a la información y apoyo logístico**

1. Los Estados miembros, la Comisión, el SEAE y la Secretaría General del Consejo velarán por que el REUE tenga acceso a cualquier información pertinente.
2. Las delegaciones de la Unión en la región y los Estados miembros, según proceda, facilitarán apoyo logístico en la región.

*Artículo 10***Seguridad**

De conformidad con la política de la Unión sobre la seguridad del personal desplegado fuera de la Unión en capacidad operativa al amparo del título V del Tratado, el REUE tomará todas las medidas razonables, de conformidad con su mandato y con la situación de la seguridad de su zona geográfica de responsabilidad, para garantizar la seguridad de todo el personal que se halle bajo su autoridad directa, en particular:

- a) estableciendo un plan de seguridad específico de la misión basado en el asesoramiento del SEAE que incluya medidas de seguridad físicas, organizativas y de procedimiento específicas de la misión, que regulen la gestión de los desplazamientos seguros del personal a la zona de la misión y dentro de ella, así como la gestión de los incidentes de seguridad, e incluya un plan de contingencia y un plan de evacuación de la misión;
- b) garantizando que todo el personal que desempeñe sus funciones fuera de la Unión esté cubierto por los seguros de alto riesgo que correspondan a las condiciones de la zona en que se realice la misión;
- c) garantizando que todos los miembros de su equipo que desempeñen sus funciones fuera de la Unión, incluido el personal local contratado, hayan recibido la formación adecuada en relación con la seguridad antes de llegar a la zona en que se realice la misión o inmediatamente después de hacerlo, en función de los índices de riesgo que el SEAE haya asignado a la zona de la misión;
- d) garantizando la aplicación de todas las recomendaciones que se deriven de las evaluaciones periódicas de seguridad y facilitando informes escritos al Consejo, a la Alta Representante y a la Comisión sobre dicha aplicación y sobre otras cuestiones relativas a la seguridad, en el marco de los informes de situación y de ejecución del mandato.

*Artículo 11***Informes**

1. Periódicamente, el REUE presentará informes orales y escritos a la Alta Representante y al CPS. En caso necesario, el REUE también informará a los grupos de trabajo del Consejo. Los informes periódicos se transmitirán a través de la red COREU. El REUE podrá presentar informes al Consejo de Asuntos Exteriores. De conformidad con el artículo 36 del Tratado, el REUE podrá tomar parte en informar al Parlamento Europeo.
2. El REUE informará sobre la manera más adecuada de realizar las iniciativas de la Unión, tales como la contribución de la Unión a reformas, incluidos los aspectos políticos de los proyectos de desarrollo de la Unión pertinentes, en coordinación con las delegaciones de la Unión en la región.

*Artículo 12***Coordinación**

1. El REUE contribuirá a la unidad, la coherencia y la eficacia de las acciones de la Unión y ayudará a garantizar que todos los instrumentos de la Unión y la acción de los Estados miembros se apliquen de manera coherente, a fin de lograr los objetivos políticos de la Unión. Las actividades del REUE se coordinarán con las de las delegaciones de la Unión y con las actividades de la Comisión. El REUE ofrecerá periódicamente sesiones de información dirigidas a las misiones de los Estados miembros y a las delegaciones de la Unión en la región.
2. Sobre el terreno, se mantendrá una estrecha relación con los Jefes de delegaciones de la Unión y con los Jefes de Misión de los Estados miembros. Estos harán todo lo posible para ayudar al REUE en la ejecución de su mandato. El REUE, en estrecha colaboración con las delegaciones de la Unión pertinentes, aportará orientaciones sobre política local al Comandante de la Fuerza de EUNAVFOR Atalanta, al Comandante de la Misión de la UE de EUTM Somalia y al Jefe de la Misión EUCAP NESTOR. El REUE, los comandantes de la operación de la UE y el Comandante civil de la operación se consultarán entre sí cuando sea necesario.

3. El REUE cooperará estrechamente con las autoridades de los países interesados, la ONU, la UA, la IGAD, otros actores nacionales, regionales e internacionales, así como con la sociedad civil de la región.

*Artículo 13*

**Revisión**

Se revisará periódicamente la ejecución de la presente Decisión y su coherencia con las demás contribuciones de la Unión a la región. El REUE presentará al Consejo, a la AR y a la Comisión un informe global sobre la ejecución de su mandato a más tardar el 31 de agosto de 2015.

*Artículo 14*

**Entrada en vigor**

La presente Decisión entrará en vigor en la fecha de su adopción.

Será de aplicación a partir del 1 de marzo de 2015.

Hecho en Bruselas, el 16 de marzo de 2015.

*Por el Consejo*

*La Presidenta*

F. MOGHERINI

---

**DECISIÓN (PESC) 2015/441 DEL CONSEJO****de 16 de marzo de 2015****por la que se modifica y prorroga la Decisión 2010/96/PESC relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas de seguridad somalíes**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, su artículo 42, apartado 4, y su artículo 43, apartado 2,

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

Considerando lo siguiente:

- (1) El 15 de febrero de 2010 el Consejo adoptó la Decisión 2010/96/PESC <sup>(1)</sup>. El mandato de la misión militar de la UE termina el 31 de marzo de 2015.
- (2) La Conferencia de Bruselas sobre Somalia, que se celebró el 16 de septiembre de 2013, sirvió de base para el Pacto sobre Somalia y puso en marcha un mecanismo para la coordinación y la responsabilización de Somalia a través del Grupo de trabajo «Nuevo Pacto» para Somalia.
- (3) Durante la reunión internacional organizada conjuntamente por el Reino Unido y Somalia, celebrada en Londres el 18 de septiembre de 2014, el Gobierno Federal presentó la vía hacia el desarrollo del Ejército Nacional Somalí hasta 2019, elaborada por el Ministerio de Defensa, y sus necesidades inmediatas.
- (4) A raíz de la revisión estratégica llevada a cabo en octubre de 2014, el mandato de la misión militar de la UE debe prorrogarse hasta el 31 de diciembre de 2016.
- (5) De conformidad con el artículo 5 del Protocolo nº 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la elaboración y aplicación de decisiones y acciones de la Unión con implicaciones en el ámbito de la defensa. Dinamarca no participa en la aplicación de la presente Decisión y, por consiguiente, no contribuye a la financiación de la presente misión.
- (6) Debe prorrogarse nuevamente el mandato de la misión militar de la UE con un mandato adaptado.

HA ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

La Decisión 2010/96/PESC se modifica como sigue:

- 1) En el artículo 1, el apartado 2 se sustituye por el texto siguiente:

«2. Con objeto de alcanzar los objetivos establecidos en el apartado 1, se desplegará la misión militar de la UE en Somalia con el fin de abordar tanto la creación de instituciones en el sector de la defensa a través de asesoramiento estratégico, como el apoyo directo al Ejército Nacional Somalí a través de la formación, del asesoramiento y de la tutoría. La misión militar de la UE estará dispuesta además a proporcionar apoyo, en consonancia con sus medios y capacidades, a otros interlocutores de la Unión en la ejecución de sus mandatos respectivos en el ámbito de la seguridad y la defensa en Somalia.»

- 2) El artículo 3 se sustituye por el texto siguiente:

*«Artículo 3***Designación del cuartel general de la misión**

1. El cuartel general de la misión estará situado en Somalia, en el Aeropuerto Internacional de Mogadiscio en Mogadiscio. Desempeñará sus funciones como cuartel general operativo y como cuartel general de la fuerza de la Unión.
2. El cuartel general de la misión incluirá una oficina de enlace y apoyo en Nairobi y una célula de apoyo en Bruselas.»

<sup>(1)</sup> Decisión 2010/96/PESC del Consejo, de 15 de febrero de 2010, relativa a una misión militar de la Unión Europea destinada a contribuir a la formación de las fuerzas de seguridad somalíes (DO L 44 de 19.2.2010, p. 16).

3) En el artículo 7, el apartado 4 se sustituye por el texto siguiente:

«4. La misión militar de la UE trabajará, dentro de los límites de sus medios y de sus capacidades, en estrecha cooperación con otros interlocutores internacionales en la región, en particular las Naciones Unidas y la AMISOM, de conformidad con los requisitos que se acuerden con el Gobierno Federal de Somalia.».

4) En el artículo 10, se añade el apartado siguiente:

«5. El importe de referencia financiera para los costes comunes de la misión militar de la UE para el período comprendido entre el 1 de abril de 2015 y el 31 de diciembre de 2016 será de 17 507 399 EUR. El porcentaje de este importe de referencia previsto en el artículo 25, apartado 1, de la Decisión ATHENA será del 30 % y el porcentaje de compromisos a que se refiere el artículo 32, apartado 3, de la Decisión ATHENA será del 90 %.».

5) Se inserta el artículo siguiente:

«Artículo 10 ter

#### **Célula de proyectos**

1. La misión militar de la UE tendrá una célula de proyectos para identificar y ejecutar proyectos, que serán financiados por los Estados miembros o terceros Estados que sean compatibles con los objetivos de la misión y contribuyan al logro del mandato.

2. Con sujeción al apartado 3, el comandante de la misión de la UE estará autorizado a recurrir a las contribuciones financieras de los Estados miembros o de terceros Estados para ejecutar proyectos identificados como complemento de otras acciones de la misión militar de la UE de manera coherente. En tal caso, el comandante de la misión de la UE celebrará un acuerdo con dichos Estados, en particular sobre los procedimientos específicos para tratar cualquier reclamación procedente de terceros por daños causados como consecuencia de los actos u omisiones del comandante de la misión de la UE en el uso de los fondos proporcionados por dichos Estados.

En ningún caso la Unión o la AR podrán ser considerados responsables por los Estados contribuyentes como consecuencia de los actos u omisiones del comandante de la misión de la UE en el uso de los fondos proporcionados por dichos Estados.

3. El CPS deberá dar su visto bueno a la aceptación de una contribución financiera de terceros Estados a la célula de proyectos.».

6) El artículo 11 se modifica como sigue:

a) en el apartado 1, la frase introductoria se sustituye por: «Se autoriza a la AR a comunicar a los Estados terceros asociados a la presente Decisión, si procede y según las necesidades de la misión, informaciones clasificadas de la UE establecidas a los fines de la misión, de conformidad con la Decisión 2013/488/UE del Consejo (\*).

(\*) Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).»;

b) en los apartados 2 y 3, los términos «Decisión 2011/292/UE» se sustituirán por «Decisión 2013/488/UE».

7) En el artículo 12, los apartados 2 y 3, se sustituyen por los siguientes:

«2. El mandato de la misión militar de la UE terminará el 31 de diciembre de 2016.

3. La presente Decisión quedará derogada a partir de la fecha de cierre del cuartel general de la misión de la UE, de la oficina de enlace y apoyo en Nairobi y de la célula de apoyo en Bruselas, de conformidad con los planes aprobados para la terminación de la misión militar de la UE, y sin perjuicio de los procedimientos relativos a la auditoría y la presentación de cuentas de la misión militar de la UE, establecidos en ATHENA.».

#### *Artículo 2*

La presente Decisión entrará en vigor el día de su adopción.

La presente Decisión será aplicable a partir del 1 de abril de 2015.

Hecho en Bruselas, el 16 de marzo de 2015.

*Por el Consejo*  
*La Presidenta*  
F. MOGHERINI



**DECISIÓN (PESC) 2015/442 DEL CONSEJO****de 16 de marzo de 2015****por la que se inicia una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUMAM RCA), y se modifica la Decisión (PESC) 2015/78**

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, sus artículos 42, apartado 4, y 43, apartado 2,

Vista la Decisión (PESC) 2015/78 del Consejo, de 19 de enero de 2015, relativa a una Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana (EUMAM RCA) <sup>(1)</sup>, y, en particular, su artículo 4,

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

Considerando lo siguiente:

- (1) El 19 de enero de 2015, el Consejo adoptó la Decisión (PESC) 2015/78.
- (2) El 9 de febrero de 2015, el Consejo aprobó las reglas de enfrentamiento de la EUMAM RCA.
- (3) El 6 de marzo de 2015, el Consejo aprobó el plan de la misión de la EUMAM RCA.
- (4) El 11 de marzo de 2015, el Comité Político y de Seguridad acogió con satisfacción la carta del comandante de la misión con la recomendación de iniciar la EUMAM RCA y el calendario previsto para declarar la capacidad operativa inicial de la EUMAM RCA.
- (5) La EUMAM RCA deber iniciarse el 16 de marzo de 2015.
- (6) De conformidad con el artículo 5 del Protocolo n° 22 sobre la posición de Dinamarca anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la elaboración y aplicación de decisiones y acciones de la Unión con implicaciones en el ámbito de la defensa. Por lo tanto, Dinamarca no participa en la aplicación de la presente Decisión, y, por consiguiente, no participa en la financiación de la presente misión.

HA ADOPTADO LA PRESENTE DECISIÓN:

*Artículo 1*

La Misión de Asesoramiento Militar PCSD de la Unión Europea en la República Centroafricana («EUMAM RCA») se iniciará el 16 de marzo de 2015.

*Artículo 2*

El comandante de la misión de la UE EUMAM RCA queda autorizado con efecto inmediato para empezar la ejecución de la misión.

*Artículo 3*

El artículo 4, apartado 2, de la Decisión (PESC) 2015/78, se sustituye por lo siguiente:

- «2. La EUMAM RCA se iniciará mediante una Decisión del Consejo en la fecha recomendada por el comandante de la misión, tras la aprobación del plan de la misión y, si es necesario, de reglas de enfrentamiento adicionales.».

<sup>(1)</sup> DO L 13 de 20.1.2015, p. 8.

*Artículo 4*

La presente Decisión entrará en vigor el día de su adopción.

Hecho en Bruselas, el 16 de marzo de 2015.

*Por el Consejo*  
*La Presidenta*  
F. MOGHERINI

---

**DECISIÓN (UE, Euratom) 2015/443 DE LA COMISIÓN**  
**de 13 de marzo de 2015**  
**sobre la seguridad en la Comisión**

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 249,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica,

Visto el Protocolo nº 7 sobre los privilegios y las inmunidades de la Unión Europea anejo a los Tratados y, en particular, su artículo 18,

Considerando lo siguiente:

- (1) El objetivo de la seguridad en la Comisión es permitir que esta pueda funcionar en un entorno seguro mediante la adopción de un planteamiento coherente e integrado por lo que respecta a su seguridad, aportando niveles adecuados de protección para las personas, los bienes y la información que sean proporcionados a los riesgos identificados, y garantizando una administración eficiente y puntual de la seguridad.
- (2) La Comisión, al igual que otros organismos internacionales, ha de hacer frente a las principales amenazas y retos en el ámbito de la seguridad, en particular en relación con el terrorismo, los ataques informáticos y el espionaje político y comercial.
- (3) La Comisión Europea ha suscrito instrumentos sobre cuestiones de seguridad para sus sedes principales con los gobiernos de Bélgica, Luxemburgo e Italia <sup>(1)</sup>. Estos instrumentos confirman que la Comisión es responsable de su seguridad.
- (4) A fin de garantizar la seguridad de las personas, los bienes y la información, la Comisión puede tener que tomar medidas en ámbitos protegidos por los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales y en el Convenio Europeo de Derechos Humanos, y reconocidos por el Tribunal de Justicia de la Unión Europea.
- (5) Cualquier medida de este tipo debe estar, por tanto, justificada por la importancia de los intereses que debe proteger, ser proporcionada y garantizar el pleno respeto de los derechos fundamentales, en particular el derecho a la intimidad y la protección de datos.
- (6) En el marco de un sistema comprometido con el Estado de Derecho y el respeto de los derechos fundamentales, la Comisión tiene que ofrecer un nivel de seguridad adecuado a su personal, bienes e información que garantice que pueda llevar a cabo sus operaciones sin limitar los derechos fundamentales más allá de lo estrictamente necesario.
- (7) La seguridad en la Comisión se basará en los principios de legalidad, transparencia, proporcionalidad y rendición de cuentas.
- (8) Los miembros del personal encargados de tomar medidas de seguridad no deben sufrir perjuicios derivados de sus acciones a menos que actúen fuera del ámbito de su mandato o infrinjan la ley y, por tanto, a este respecto, la presente Decisión debe considerarse como una instrucción de servicio en el sentido del Estatuto.
- (9) La Comisión deberá tomar las iniciativas adecuadas para impulsar y reforzar su cultura de seguridad, garantizando una administración de la seguridad más eficiente, mejorando la gobernanza de la seguridad, intensificando aún más las redes y la cooperación con las autoridades pertinentes a nivel internacional, europeo y nacional, y mejorando la supervisión y el control de la aplicación de las medidas de seguridad.
- (10) La creación del Servicio Europeo de Acción Exterior (SEAE) como organismo de la Unión funcionalmente autónomo ha tenido un impacto significativo en los intereses en materia de seguridad de la Comisión y, por tanto, exige que se establezcan normas y procedimientos de cooperación en lo que respecta a la seguridad y la protección entre el SEAE y la Comisión, en particular en relación con el cumplimiento de las obligaciones de asistencia y protección de la Comisión hacia su personal en las Delegaciones de la Unión.

<sup>(1)</sup> Véase el «Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité» de 31 de diciembre de 2004, el «Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois», de 20 de enero de 2007, y el «Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale», de 22 de julio de 1959.

- (11) La política de seguridad de la Comisión debe aplicarse de manera coherente con otros procesos y procedimientos internos que puedan implicar un elemento de seguridad. Se trata, en particular, de la gestión de la continuidad de las actividades, dirigida a mantener las funciones esenciales de la Comisión en caso de perturbación, y del sistema ARGUS para la coordinación multisectorial en caso de crisis.
- (12) A pesar de las medidas ya vigentes en el momento de la adopción de la presente Decisión y notificadas al Supervisor Europeo de Protección de Datos <sup>(1)</sup>, cualquier medida prevista en el marco de la presente Decisión que implique el tratamiento de datos personales estará sujeta a las normas de desarrollo de conformidad con lo dispuesto en el artículo 21, que establecerá las oportunas garantías para los interesados.
- (13) Por lo tanto, es preciso que la Comisión revise, actualice y consolide las actuales bases normativas de seguridad de la Comisión.
- (14) Por consiguiente, procede derogar la Decisión C (94)2129 de la Comisión <sup>(2)</sup>.

HA ADOPTADO LA PRESENTE DECISIÓN:

#### CAPÍTULO 1

#### DISPOSICIONES GENERALES

##### Artículo 1

#### Definiciones

A efectos de la presente Decisión, se aplicarán las siguientes definiciones:

- 1) «activos»: todos los bienes muebles e inmuebles y bienes de la Comisión;
- 2) «servicio de la Comisión»: Dirección General o servicio de la Comisión, o gabinete de un miembro de la Comisión;
- 3) «sistema de información y comunicaciones» o «SIC»: todo sistema que permita el tratamiento de información en formato electrónico, incluyendo todos los activos necesarios para su funcionamiento, así como la infraestructura, la organización, personal y recursos de información;
- 4) «control de riesgos»: cualquier medida de seguridad que pueda esperarse razonablemente que controle eficazmente un riesgo para la seguridad mediante su prevención, mitigación, evitación o transferencia;
- 5) «situación de crisis»: hecho, suceso o incidente o emergencia (o una sucesión o combinación de ellos) que presente una amenaza importante o inmediata para la seguridad en la Comisión independientemente de su origen;
- 6) «datos»: información en un formato que permita su transmisión, registro o tratamiento;
- 7) «miembro de la Comisión responsable de la seguridad»: miembro de la Comisión bajo cuya autoridad se encuentra la Dirección General de Recursos Humanos y Seguridad;
- 8) «datos personales»: datos personales tal como se definen en el artículo 2, letra a), del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo <sup>(3)</sup>;
- 9) «locales»: todo inmueble o propiedades y posesiones asimiladas de la Comisión;
- 10) «prevención de riesgos»: cualquier medida de seguridad que pueda esperarse razonablemente que obstaculice, retrase o detenga un riesgo para la seguridad;
- 11) «riesgo para la seguridad»: combinación del nivel de amenaza, el nivel de vulnerabilidad y el posible impacto de un suceso;
- 12) «seguridad en la Comisión»: seguridad de las personas, los bienes y la información de la Comisión y, en particular, la integridad física de las personas y los bienes, la integridad, confidencialidad y disponibilidad de la información y de los sistemas de comunicación e información, así como el libre funcionamiento de las operaciones de la Comisión;

<sup>(1)</sup> DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

<sup>(2)</sup> Decisión C (94) 2129 de la Comisión, de 8 de septiembre de 1994, relativa a las tareas de la Oficina de Seguridad.

<sup>(3)</sup> Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

- 13) «medida de seguridad»: cualquier medida adoptada de conformidad con la presente Decisión a efectos de controlar los riesgos para la seguridad;
- 14) «Estatuto de los funcionarios»: el Estatuto de los funcionarios de la Unión Europea, establecido por el Reglamento (CEE, Euratom, CECA) n° 259/68 del Consejo <sup>(1)</sup> y sus actos modificativos;
- 15) «amenaza para la seguridad»: suceso o agente que pueda esperarse razonablemente que afecte negativamente a la seguridad en caso de no ser abordado y controlado;
- 16) «amenaza inmediata para la seguridad»: amenaza para la seguridad que se produce sin previo aviso o con previo aviso extremadamente corto;
- 17) «amenaza grave para la seguridad»: amenaza para la seguridad que pueda razonablemente esperarse que dé lugar a la pérdida de vidas, daños o lesiones graves, daños materiales importantes, la puesta en peligro de información muy sensible, o perturbaciones de los sistemas informáticos o de las capacidades operativas esenciales de la Comisión;
- 18) «vulnerabilidad»: carencia, cualquiera que sea su naturaleza, que pueda razonablemente esperarse que afecte negativamente a la seguridad en la Comisión, si es aprovechada por una o varias amenazas.

## Artículo 2

### Objeto

1. La presente Decisión establece los objetivos, principios básicos, organización y responsabilidades en materia de seguridad en la Comisión.
2. La presente Decisión se aplicará a todos los servicios de la Comisión y en todos los locales de la Comisión. El personal de la Comisión que trabaje en las Delegaciones de la Unión estará sujeto a las normas de seguridad del Servicio Europeo de Acción Exterior <sup>(2)</sup>.
3. Sin perjuicio de las indicaciones específicas relativas a grupos concretos de personal, la presente Decisión se aplicará a los miembros de la Comisión, al personal de la Comisión en el ámbito de aplicación del Estatuto de los funcionarios y del Régimen aplicable a los otros agentes de la Unión Europea, a los expertos nacionales destinados en comisión de servicios a la Comisión, a los proveedores de servicios y a su personal, a los trabajadores en prácticas y a cualquier persona con acceso a los edificios u otros bienes de la Comisión, o a la información manejada por la Comisión.
4. Las disposiciones de la presente Decisión se entenderán sin perjuicio de lo dispuesto en la Decisión 2002/47/CE, CECA, Euratom de la Comisión <sup>(3)</sup>, la Decisión 2004/563/CE, Euratom de la Comisión <sup>(4)</sup>, la Decisión C(2006) 1623 de la Comisión <sup>(5)</sup> y la Decisión C(2006) 3602 de la Comisión <sup>(6)</sup>.

## CAPÍTULO 2

### PRINCIPIOS

## Artículo 3

### Principios de seguridad en la Comisión

1. Al aplicar la presente Decisión, la Comisión deberá cumplir los Tratados y, en particular, la Carta de los Derechos Fundamentales y el Protocolo n° 7 sobre los privilegios y las inmunidades de la Unión Europea; los instrumentos a que se hace referencia en el considerando 2; las normas de Derecho nacional aplicables; así como las disposiciones de la presente Decisión. En caso necesario, se emitirá un aviso de seguridad en el sentido del artículo 21, apartado 2, proporcionando directrices a este respecto.
2. La seguridad en la Comisión se basará en los principios de legalidad, transparencia, proporcionalidad y rendición de cuentas.
3. El principio de legalidad indica la necesidad de permanecer estrictamente en el marco jurídico al aplicar la presente Decisión, y la necesidad de ajustarse a los requisitos jurídicos.

<sup>(1)</sup> Reglamento (CEE, Euratom, CECA) n° 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (régimen aplicable a los otros agentes) (DO L 56 de 4.3.1968, p. 1).

<sup>(2)</sup> Decisión de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 19 de abril de 2013, sobre las normas de seguridad del Servicio Europeo de Acción Exterior (DO C 190 de 29.6.2013, p. 1).

<sup>(3)</sup> Decisión 2002/47/CE, CECA, Euratom de la Comisión, de 23 de enero de 2002, por la que se modifica su Reglamento interno (DO L 21 de 24.1.2002, p. 23), que adjunta disposiciones relativas a la gestión de documentos electrónicos y digitalizados.

<sup>(4)</sup> Decisión 2004/563/CE, Euratom de la Comisión, de 7 de julio de 2004, por la que se modifica su Reglamento interno (DO L 251 de 27.7.2004, p. 9), que adjunta disposiciones relativas a los documentos electrónicos y digitalizados.

<sup>(5)</sup> Decisión C(2006) 1623 de la Comisión, de 21 de abril de 2006, por la que se establece una política armonizada en materia de salud y seguridad en el trabajo para todo el personal de la Comisión Europea.

<sup>(6)</sup> Decisión C(2006) 3602, de 16 de agosto de 2006 de la Comisión, relativa a la seguridad de los sistemas de información utilizados por la Comisión Europea.

4. Las medidas de seguridad se tomarán de forma visible, excepto en caso de que pueda esperarse razonablemente que ello vaya en menoscabo de su efecto. Los destinatarios de una medida de seguridad deberán ser informados previamente de los motivos y los efectos de la medida, a menos que pueda esperarse razonablemente que el efecto de la medida vaya a verse afectado por la comunicación de dicha información. En este caso, el destinatario de la medida de seguridad será informado una vez haya cesado el riesgo de menoscabar el efecto de la medida de seguridad.

5. Los servicios de la Comisión velarán por que se tengan en cuenta las cuestiones de seguridad desde el inicio de la elaboración y la aplicación de las políticas, decisiones, programas, proyectos y actividades de la Comisión de las que son responsables. Para ello, se contará con la participación de la Dirección General de Recursos Humanos y Seguridad en general, y con el responsable principal de la seguridad de la información de la Comisión por lo que se refiere a los sistemas informáticos, desde las primeras fases de elaboración.

6. La Comisión, en su caso, buscará la colaboración de las autoridades competentes del Estado miembro de acogida, de otros Estados miembros y de otras instituciones, agencias u organismos de la UE, cuando sea posible, teniendo en cuenta las medidas adoptadas o previstas por dichas autoridades para abordar el riesgo para la seguridad de que se trate.

#### Artículo 4

### Obligación de cumplimiento

1. Será obligatorio el cumplimiento de la presente Decisión y de sus normas de desarrollo, así como de las medidas de seguridad y las instrucciones dadas por el personal autorizado.
2. El incumplimiento de las normas de seguridad podrá dar lugar a medidas disciplinarias de conformidad con los Tratados y el Estatuto de los funcionarios, a sanciones contractuales, o a acciones judiciales de conformidad con las disposiciones legales y reglamentarias nacionales.

#### CAPÍTULO 3

### GARANTIZAR LA SEGURIDAD

#### Artículo 5

### Personal autorizado

1. Únicamente el personal autorizado en virtud de un mandato nominativo conferido por el Director General de Recursos Humanos y Seguridad, habida cuenta de sus funciones, tendrá la facultad para adoptar una o varias de las medidas siguientes:
  - 1) portar armas de mano;
  - 2) realizar las investigaciones de seguridad a que se refiere el artículo 13;
  - 3) tomar las medidas de seguridad a que se refiere el artículo 12, según se especifique en el mandato.
2. El mandato a que se refiere el apartado 1 se conferirá por un período que no podrá exceder del período durante el cual la persona en cuestión ejerza el cargo o función en relación con el cual le haya sido atribuido el mandato. Los mandatos se conferirán en cumplimiento de las disposiciones aplicables establecidas en el artículo 3, apartado 1.
3. Por lo que se refiere al personal autorizado, la presente Decisión constituye una instrucción de servicio en el sentido del artículo 21 del Estatuto de los funcionarios.

#### Artículo 6

### Disposiciones generales relativas a las medidas de seguridad

1. Al adoptar medidas de seguridad, la Comisión garantizará en particular, en la medida en que razonablemente sea posible, que:
  - a) Solo buscará apoyo o asistencia del Estado de que se trate siempre que dicho Estado sea un Estado miembro de la Unión Europea o, de no serlo, sea parte en el Convenio Europeo de Derechos Humanos, o garantice derechos que sean al menos equivalentes a los que garantiza este Convenio.
  - b) Solo transmitirá información relativa a un individuo a destinatarios distintos de las instituciones y los organismos comunitarios, que no estén sujetos al Derecho nacional adoptado en aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo <sup>(1)</sup>, de conformidad con el artículo 9 del Reglamento (CE) n° 45/2001.

<sup>(1)</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

- c) Cuando una persona constituya una amenaza para la seguridad, podrán aplicársele medidas de seguridad y esa persona podrá tener que asumir los costes correspondientes. Dichas medidas de seguridad solo podrán dirigirse contra otras personas si debe controlarse una amenaza inmediata o grave para la seguridad y se cumplen las condiciones siguientes:
- las medidas previstas contra la persona que supone la amenaza para la seguridad no pueden adoptarse o no es probable que sean eficaces;
  - la Comisión no puede controlar la amenaza para la seguridad a través de sus propias acciones o no puede hacerlo a su debido tiempo;
  - la medida no constituye un peligro desproporcionado para otras personas y sus derechos.
2. La Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad elaborará un compendio de las medidas de seguridad que pueden requerir una orden judicial de conformidad con las disposiciones legales y reglamentarias de los Estados miembros que acogen a los locales de la Comisión.
3. La Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad podrá recurrir a un contratista para que realice, bajo la dirección y supervisión de la Dirección de Seguridad, funciones relacionadas con la seguridad.

#### Artículo 7

##### **Medidas de seguridad en relación con las personas**

- Deberá otorgarse un nivel adecuado de protección a las personas en los locales de la Comisión, teniendo en cuenta los requisitos de seguridad y protección.
- En caso de riesgos importantes para la seguridad, la Dirección General de Recursos Humanos y Seguridad proporcionará protección personal a los miembros de la Comisión u otros miembros del personal, cuando una evaluación de las amenazas indique que tal medida es necesaria para garantizar su seguridad y protección.
- En caso de riesgos importantes para la seguridad, la Comisión podrá ordenar la evacuación de sus locales.
- Las víctimas de accidentes o ataques en los locales de la Comisión recibirán ayuda.
- Con el fin de prevenir y controlar los riesgos para la seguridad, el personal autorizado podrá llevar a cabo comprobaciones de los antecedentes personales de las personas comprendidas en el ámbito de aplicación de la presente Decisión, con el fin de determinar si facilitar a dichas personas el acceso a los locales o información de la Comisión representa una amenaza para la seguridad. Con este fin, y de conformidad con el Reglamento (CE) nº 45/2001 y las disposiciones a que se refiere el artículo 3, apartado 1, el personal autorizado en cuestión podrá:
  - utilizar cualquier fuente de información de que dispone la Comisión, teniendo en cuenta la fiabilidad de la fuente de información;
  - acceder al expediente o los datos que posea la Comisión respecto de las personas que emplea, o pretende emplear, o del personal de los contratistas cuando esté debidamente justificado.

#### Artículo 8

##### **Medidas de seguridad en relación con la seguridad física y los bienes**

- La seguridad de los bienes debe garantizarse mediante la aplicación de medidas de protección físicas y técnicas adecuadas y los procedimientos correspondientes, que en lo sucesivo se denominarán «seguridad física», creando un sistema con múltiples capas.
- Se podrán adoptar medidas en virtud del presente artículo, con el fin de proteger a las personas o la información y los bienes de la Comisión.
- La seguridad física tendrá los siguientes objetivos:
  - prevenir actos de violencia dirigidos contra los miembros de la Comisión o las personas que entran en el ámbito de aplicación de la presente Decisión,
  - prevenir el espionaje y las escuchas indebidas de información sensible o clasificada,
  - prevenir robos, actos de vandalismo, sabotaje y otras acciones violentas destinadas a perjudicar o destruir edificios y bienes de la Comisión,

- permitir la investigación de los incidentes de seguridad, en particular mediante la verificación de los registros de controles de acceso y salida, los circuitos cerrados de televisión, las grabaciones de llamadas telefónicas y datos similares a que se refiere el artículo 22, apartado 2, y otras fuentes de información.
4. La seguridad física incluirá:
- una política de acceso aplicable a cualquier persona o vehículo que requiera acceso a los locales de la Comisión, incluidos los aparcamientos,
  - un sistema de control de acceso que incluya guardas, medidas y equipos técnicos, sistemas de información o una combinación de todos estos elementos.
5. Con el fin de garantizar la seguridad física, podrán adoptarse las siguientes medidas:
- registrar la entrada y salida de los locales de la Comisión de personas, vehículos, equipos y bienes,
  - realizar controles de identidad en los locales,
  - inspeccionar vehículos, bienes y equipos por medios visuales o técnicos,
  - impedir que personas, vehículos y equipos no autorizados entren en los locales de la Comisión.

#### Artículo 9

### Medidas de seguridad en relación con la información

1. La seguridad de la información se refiere a toda la información manejada por la Comisión.
2. La seguridad de la información, con independencia de su forma, deberá ponderar la transparencia, proporcionalidad, responsabilidad y eficiencia frente a la necesidad de proteger la información contra el acceso, uso, divulgación, modificación o destrucción no autorizados.
3. La seguridad de la información tendrá por objetivo proteger su confidencialidad, integridad y disponibilidad.
4. Los procesos de gestión de riesgos deberán utilizarse por tanto para clasificar los activos de información y desarrollar normas, procedimientos y medidas de seguridad proporcionadas, en particular medidas paliativas.
5. Estos principios generales de seguridad de la información se aplicarán, en particular, en lo que se refiere a:
  - a) «Información clasificada de la Unión Europea» (en lo sucesivo, «ICUE»), es decir, toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios de sus Estados miembros.
  - b) «Información sensible no clasificada», es decir, información o material que la Comisión debe proteger por razón de obligaciones legales establecidas en los Tratados o en actos adoptados en aplicación del mismo, o por razón de su carácter sensible. La información sensible no clasificada incluye, pero no se limita a, la información o el material cubiertos por la obligación de secreto profesional, en virtud de lo dispuesto en el artículo 339 del TFUE; la información cubierta por los intereses protegidos en el artículo 4 del Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo <sup>(1)</sup> leído en relación con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea; o los datos personales incluidos en el ámbito de aplicación del Reglamento (CE) n° 45/2001.
6. La información sensible no clasificada estará sujeta a las normas relativas a su manejo y almacenamiento. Solo se revelará a los individuos que tienen «necesidad de conocer». Cuando se considere necesario para la protección efectiva de su confidencialidad, se identificará mediante un marcado de seguridad y las correspondientes instrucciones de manejo aprobadas por el director general de Recursos Humanos y Seguridad. Cuando se maneje o almacene en sistemas de comunicación e información, dicha información deberá también ser protegida de conformidad con la Decisión C(2006) 3602, sus normas de desarrollo y las normas correspondientes.
7. Toda persona que sea responsable de comprometer o perder ICUE o información sensible no clasificada, identificada como tal en las normas relativas a su manejo y almacenamiento, podrá ser objeto de medidas disciplinarias de conformidad con el Estatuto de los funcionarios. Tales medidas disciplinarias se entenderán sin perjuicio de cualquier otro proceso judicial o penal por parte de las autoridades nacionales competentes de los Estados miembros de conformidad con sus disposiciones legales y reglamentarias, y de los instrumentos contractuales.

<sup>(1)</sup> Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).



*Artículo 10***Medidas de seguridad en relación con los sistemas de información y comunicación**

1. Todos los sistemas de información y comunicación (en lo sucesivo, «SIC») utilizados por la Comisión se ajustarán a la política de seguridad de los sistemas de información de la Comisión, tal como se establece en la Decisión C(2006) 3602, sus normas de desarrollo y las correspondientes normas de seguridad.
2. Los servicios de la Comisión que posean, gestionen u operen SIC únicamente permitirán a otras instituciones, agencias, órganos de la Unión o a otras organizaciones el acceso a estos sistemas siempre que dichas instituciones, agencias, órganos de la Unión u otras organizaciones puedan ofrecer garantías razonables de que sus sistemas informáticos están protegidos a un nivel equivalente al que ofrece la política de seguridad de los sistemas de información de la Comisión, tal como se establece en la Decisión C(2006) 3602, sus normas de desarrollo y las correspondientes normas de seguridad. La Comisión supervisará dicho cumplimiento, y, en caso de incumplimiento grave o persistente, podrá prohibir el acceso.

*Artículo 11***Análisis forense sobre ciberseguridad**

La Dirección General de Recursos Humanos y Seguridad será responsable, en particular, de realizar análisis técnicos forenses en cooperación con los servicios competentes de la Comisión en apoyo de las investigaciones de seguridad a que se hace referencia en el artículo 13, en relación con el contraespionaje, la filtración de datos, los ciberataques y la seguridad de los sistemas de información.

*Artículo 12***Medidas de seguridad en lo que respecta a personas y objetos**

1. Con el fin de garantizar la seguridad en la Comisión y prevenir y controlar los riesgos, el personal autorizado con arreglo al artículo 5 podrá, de conformidad con los principios enunciados en el artículo 3, adoptar, entre otras, una o más de las siguientes medidas de seguridad:
  - a) aseguramiento de lugares y pruebas, incluidos los registros de controles de acceso y salida y las imágenes de circuito cerrado de televisión, en caso de incidentes o de actuaciones que puedan dar lugar a procedimientos administrativos, disciplinarios, civiles o penales;
  - b) medidas limitadas en relación con personas que supongan una amenaza para la seguridad, en particular ordenar a las personas que abandonen los locales de la Comisión, acompañar a las personas que salgan de los locales de la Comisión, prohibir el acceso de personas a los locales de la Comisión durante un período de tiempo, definiéndose esto último de conformidad con los criterios que se establezcan en las normas de desarrollo;
  - c) medidas limitadas con respecto a los objetos que supongan una amenaza para la seguridad, en particular su retirada, incautación y eliminación;
  - d) registros en los locales de la Comisión, incluso de despachos, dentro de dichos locales;
  - e) registro en SIC y equipos, datos de tráfico de teléfono y de telecomunicaciones, archivos de registros, cuentas de usuario, etc.;
  - f) otras medidas de seguridad específicas con efectos similares a fin de prevenir o controlar los riesgos para la seguridad, en particular, en el contexto de los derechos de la Comisión como propietario o empleador, de conformidad con la legislación nacional aplicable.
2. En circunstancias excepcionales, los miembros del personal de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad, mandatados de conformidad con el artículo 5, podrán tomar las medidas urgentes necesarias, en el estricto respeto de los principios enunciados en el artículo 3. Lo antes posible, tras haber adoptado estas medidas, informarán al director de la Dirección de Seguridad, que solicitará el mandato pertinente del director general de la Dirección General de Recursos Humanos y Seguridad confirmando las medidas adoptadas y autorizando cualquier otra acción necesaria, y se mantendrán en contacto, en su caso, con las autoridades nacionales competentes.
3. Las medidas de seguridad de conformidad con el presente artículo se documentarán en el momento en que se tomen o, en caso de riesgo inmediato o situación de crisis, en un plazo razonable después de que se hayan tomado. En este último caso, la documentación deberá incluir también los elementos en que se base la apreciación relativa a la existencia de un riesgo inmediato o una situación de crisis. La documentación podrá ser sucinta, pero deberá estar elaborada de tal manera que permita a la persona objeto de la medida ejercer sus derecho de defensa y protección de los datos personales de conformidad con el Reglamento (CE) n° 45/2001, y permitir un control de la legalidad de la medida. Ninguna información relativa a las medidas específicas de seguridad dirigidas a un miembro del personal formará parte del expediente personal del interesado.

4. Al adoptar medidas de seguridad con arreglo a la letra b), la Comisión deberá, además, garantizar que la persona de que se trate tenga la posibilidad de ponerse en contacto con un abogado o una persona de su confianza y tener conocimiento de su derecho a recurrir al Supervisor Europeo de Protección de Datos.

#### Artículo 13

##### Investigaciones

1. Sin perjuicio de lo dispuesto en el artículo 86 y el anexo IX del Estatuto de los funcionarios, y de cualquier régimen especial entre la Comisión y el SEAE, como el régimen especial firmado el 28 de mayo de 2014 entre la Dirección General de Recursos Humanos y Seguridad de la Comisión Europea y el Servicio Europeo de Acción Exterior sobre las obligaciones de asistencia y protección hacia el personal de la Comisión destinado en las Delegaciones de la Unión, podrán realizarse investigaciones de seguridad:

- a) en caso de incidentes que afecten a la seguridad de la Comisión, incluida la sospecha de infracciones penales;
- b) en caso de posibles fugas, mal manejo o peligro de la información sensible no clasificada, la ICUE o la información clasificada de Euratom;
- c) en el contexto de la contrainteligencia y la lucha contra el terrorismo;
- d) en caso de ciberincidentes graves.

2. La decisión de llevar a cabo una investigación de seguridad será adoptada por el director general de la Dirección General de Recursos Humanos y Seguridad, que también será el destinatario del informe de investigación.

3. Las investigaciones de seguridad las realizarán únicamente miembros específicos del personal de la Dirección General de Recursos Humanos y Seguridad, debidamente autorizados de conformidad con el artículo 5.

4. El personal autorizado ejercerá sus competencias de investigación de seguridad de forma independiente, tal como se especifica en el mandato, y asumirá las competencias enumeradas en el artículo 12.

5. El personal autorizado con competencia para realizar investigaciones de seguridad podrá recabar información de todas las fuentes disponibles en relación con cualquier infracción administrativa o penal cometida en los locales de la Comisión o en relación con las personas a que se hace referencia en el artículo 2, apartado 3, ya sea como víctimas o como autores de dichas infracciones.

6. La Dirección General de Recursos Humanos y Seguridad informará de ello a las autoridades competentes del Estado miembro de acogida o de cualquier otro Estado miembro interesado, cuando proceda y, en particular, en caso de que la investigación haya aportado indicios de que se ha cometido una infracción penal. En este contexto, cuando lo considere apropiado o sea requerida para ello, la Dirección General de Recursos Humanos y Seguridad podrá prestar asistencia a las autoridades del Estado miembro de acogida o de cualquier otro Estado miembro interesado.

7. En el caso de ciberincidentes graves, la Dirección General de Informática colaborará estrechamente con la Dirección General de Recursos Humanos y Seguridad para apoyarla en todas las cuestiones técnicas. La Dirección General de Recursos Humanos y Seguridad decidirá, en consulta con la Dirección General de Informática, cuándo es oportuno informar a las autoridades competentes del país de acogida o de cualquier otro Estado miembro interesado. Los servicios de coordinación de incidentes del equipo de respuesta a emergencias informáticas de las instituciones, órganos y agencias de la Unión Europea (en lo sucesivo, «CERT») podrán ayudar a otras instituciones y agencias de la UE que puedan verse afectadas.

8. Las investigaciones de seguridad deberán estar documentadas.

#### Artículo 14

##### Delimitación de competencias con respecto a las investigaciones de seguridad y otros tipos de investigaciones

1. Cuando la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad lleve a cabo investigaciones de seguridad, tal como se contempla en el artículo 13, y si estas investigaciones entran dentro de las competencias de la Oficina Europea de Lucha contra el Fraude (OLAF) o la Oficina de Investigación y Disciplina de la Comisión (IDOC), se pondrá en contacto con dichos organismos de forma inmediata con el fin, en particular, de no comprometer las gestiones posteriores de la OLAF y la IDOC. Cuando proceda, la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad invitará a la OLAF o a la IDOC a que participen en la investigación.

2. Las investigaciones de seguridad a que se refiere el artículo 13 se entenderán sin perjuicio de las competencias de la OLAF y la IDOC según lo dispuesto en los reglamentos aplicables a dichas oficinas. Podrá pedirse a la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad que proporcione asistencia técnica a las investigaciones abiertas por la OLAF o la IDOC.

3. Podrá pedirse a la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad que asista a los agentes de la OLAF cuando accedan a los locales de la Comisión de conformidad con el artículo 3, apartado 5, y el artículo 4, apartado 4, del Reglamento (UE, Euratom) n° 883/2013 del Parlamento Europeo y del Consejo <sup>(1)</sup>, con el fin

<sup>(1)</sup> Reglamento (UE, Euratom) n° 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF) y por el que se deroga el Reglamento (CE) n° 1073/1999 del Parlamento Europeo y del Consejo y el Reglamento (Euratom) n° 1074/1999 del Consejo (DO L 248 de 18.9.2013, p. 1).

de facilitar su labor. La Dirección de Seguridad informará de tales solicitudes de asistencia al secretario general y al director general de la Dirección General de Recursos Humanos y Seguridad o, si dicha investigación se realiza en locales de la Comisión ocupados por sus miembros o por el secretario general, al presidente de la Comisión y al comisario responsable de recursos humanos.

4. Sin perjuicio de lo dispuesto en el artículo 22, letra a), del Estatuto, cuando un asunto pueda entrar en el ámbito de competencias tanto de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad como de la IDOC, la Dirección de Seguridad deberá, cuando responda ante el director general de Recursos Humanos y Seguridad de conformidad con el artículo 13 en la fase más temprana posible, advertir si existen razones que justifiquen que la IDOC se encargue del asunto. En particular, esta fase se considerará alcanzada cuando haya finalizado una amenaza inmediata a la seguridad. El director general de la Dirección General de Recursos Humanos y Seguridad decidirá al respecto.

5. Si un asunto puede entrar en el ámbito de competencias tanto de la Dirección de Seguridad de la Dirección General de Recursos Humanos y Seguridad como de la OLAF, la Dirección de Seguridad lo notificará sin demora al director general de la Dirección General de Recursos Humanos y Seguridad e informará al director general de la OLAF lo antes posible. En particular, esta fase se considerará alcanzada cuando haya finalizado una amenaza inmediata a la seguridad.

#### Artículo 15

### Inspecciones de seguridad

1. La Dirección General de Recursos Humanos y Seguridad realizará las inspecciones de seguridad para comprobar el cumplimiento por parte de los servicios de la Comisión y los particulares de la presente Decisión y sus normas de desarrollo, y formular recomendaciones cuando se considere necesario.

2. En su caso, la Dirección General de Recursos Humanos y Seguridad llevará a cabo las inspecciones de seguridad o el control de la seguridad o las visitas de evaluación a fin de comprobar si la seguridad del personal, activos e información de la Comisión que sea responsabilidad de otras instituciones, órganos u organismos de la Unión, Estados miembros, terceros Estados u organizaciones internacionales, está adecuadamente protegida de conformidad con normas y reglamentaciones de seguridad que sean, como mínimo, equivalentes a las de la Comisión. En caso necesario y en un espíritu de buena cooperación entre administraciones, esas inspecciones de seguridad incluirán también inspecciones realizadas en el contexto del intercambio de información clasificada con otras instituciones, organismos y agencias de la Unión, Estados miembros, o con terceros Estados u organizaciones internacionales.

3. Este artículo se aplicará, *mutatis mutandis*, al personal de la Comisión en las Delegaciones de la Unión, sin perjuicio de cualquier régimen especial entre la Comisión y el SEAE, como el acuerdo especial firmado el 28 de mayo de 2014 entre la Dirección General de Recursos Humanos y Seguridad de la Comisión Europea y el Servicio Europeo de Acción Exterior sobre las obligaciones de asistencia y protección hacia el personal de la Comisión destinado en las Delegaciones de la Unión.

#### Artículo 16

### Estados de alerta y gestión de situaciones de crisis

1. La Dirección General de Recursos Humanos y Seguridad será responsable de poner en marcha medidas de alerta adecuadas en previsión de o en respuesta a amenazas e incidentes que afecten a la seguridad de la Comisión, y las medidas necesarias para gestionar situaciones de crisis.

2. Las medidas de alerta contempladas en el apartado 1 serán acordes con el nivel de amenaza para la seguridad. Los niveles de alerta deberán definirse en estrecha cooperación con los servicios competentes de otras instituciones, agencias y organismos de la Unión, y del Estado miembro o Estados miembros que acojan a los locales de la Comisión.

3. La Dirección General de Recursos Humanos y Seguridad será el punto de contacto para las alertas y la gestión de situaciones de crisis.

#### CAPÍTULO 4

### ORGANIZACIÓN

#### Artículo 17

### Responsabilidades generales de los servicios de la Comisión

1. Las responsabilidades de la Comisión a que se hace referencia en la presente Decisión serán ejercidas por la Dirección General de Recursos Humanos y Seguridad bajo la autoridad y la responsabilidad del miembro de la Comisión responsable de la seguridad.

2. Las disposiciones específicas por lo que se refiere a la seguridad cibernética se definen en la Decisión (2006)3602.
3. Las responsabilidades de la aplicación de la presente Decisión y sus normas de desarrollo, y del cumplimiento cotidiano, podrán delegarse a otros servicios de la Comisión, siempre que la descentralización de los servicios de seguridad ofrezca una considerable eficiencia o ahorro de recursos o de tiempo, por ejemplo debido a la ubicación geográfica de los servicios en cuestión.
4. En los casos en que se aplique el apartado 3, la Dirección General de Recursos Humanos y Seguridad, y, si procede, la Dirección General de Informática organizarán acuerdos con servicios concretos de la Comisión para establecer claramente las funciones y responsabilidades para la aplicación y el seguimiento de las políticas de seguridad.

#### Artículo 18

##### **Dirección General de Recursos Humanos y Seguridad**

1. La Dirección General de Recursos Humanos y Seguridad será responsable, en particular, de:
  - 1) desarrollar la política de seguridad de la Comisión, las normas de desarrollo y los avisos de seguridad;
  - 2) recoger información con vistas a la evaluación de las amenazas y los riesgos para la seguridad y sobre todas las cuestiones que puedan afectar a la seguridad en la Comisión;
  - 3) proporcionar contravigilancia electrónica y protección a todos los locales de la Comisión, teniendo debidamente en cuenta las evaluaciones de amenazas y las pruebas de actividades no autorizadas contra los intereses de la Comisión;
  - 4) prestar un servicio de emergencia permanente (24 horas y 7 días a la semana) para los servicios de la Comisión y el personal respecto de cualquier cuestión relacionada con la seguridad y la protección;
  - 5) aplicar medidas de seguridad destinadas a mitigar los riesgos para la seguridad, y desarrollar y mantener SCI adecuados para cubrir sus necesidades operativas, en particular en los ámbitos del control de acceso físico, la administración de autorizaciones de seguridad y el manejo de la información sensible y clasificada de la UE;
  - 6) sensibilizar, organizar ejercicios y ofrecer formación y asesoramiento sobre todas las cuestiones relacionadas con la seguridad en la Comisión, con el fin de promover una cultura de seguridad y crear un núcleo de personal con la formación adecuada en materia de seguridad.
2. La Dirección General de Recursos Humanos y Seguridad, sin perjuicio de las competencias y responsabilidades de otros servicios de la Comisión, mantendrá un enlace externo con:
  - 1) los servicios de seguridad de otras instituciones, agencias y organismos de la Unión, sobre cuestiones relacionadas con la seguridad de las personas, los bienes y la información de la Comisión;
  - 2) los servicios de seguridad, inteligencia y evaluación de amenazas, en particular las autoridades nacionales de seguridad, de los Estados miembros, de terceros países o de organizaciones internacionales y organismos sobre cuestiones que afectan a la seguridad de las personas, los bienes y la información de la Comisión;
  - 3) la policía y otros servicios de emergencia sobre todas las cuestiones rutinarias y de emergencia que afecten a la seguridad de la Comisión;
  - 4) las autoridades de seguridad de otras instituciones de la Unión, de las agencias y organismos, de los Estados miembros y de terceros países en el ámbito de la lucha contra los ataques cibernéticos con un impacto potencial en la seguridad en la Comisión;
  - 5) en relación con la recepción, análisis y distribución de información relacionada con amenazas que plantean las actividades de espionaje y terrorismo que afectan a la seguridad en la Comisión;
  - 6) en relación con las cuestiones relativas a la información clasificada, tal como se especifica en la Decisión (UE, Euratom) 2015/444 de la Comisión <sup>(1)</sup>.
3. La Dirección General de Recursos Humanos y Seguridad será responsable de la transmisión segura de información realizada con arreglo al presente artículo, incluida la transmisión de datos personales.

#### Artículo 19

##### **Grupo de expertos de la Comisión en materia de seguridad (ComSEG)**

Se creará un grupo de expertos de la Comisión en materia de seguridad, con el mandato de asesorar a la Comisión, cuando proceda, sobre cuestiones relativas a su política de seguridad interior y, más concretamente, sobre la protección de la información clasificada de la UE.

<sup>(1)</sup> Decisión (UE, Euratom) 2015/444 de la Comisión, de 13 de marzo de 2015, sobre las normas de seguridad para la protección de la información clasificada de la UE (véase la página 53 del presente Diario Oficial).

*Artículo 20***Responsable local de seguridad (LSO)**

1. Cada servicio de la Comisión o gabinete nombrará un responsable local de seguridad (LSO), que actuará como principal punto de contacto entre el servicio y la Dirección General de Recursos Humanos y Seguridad sobre todos los asuntos relacionados con la seguridad en la Comisión. En su caso, podrán nombrarse uno o varios LSO adjuntos. El LSO será un funcionario o un agente temporal.
2. Como principal punto de contacto sobre seguridad dentro de su servicio o gabinete, el LSO informará de forma periódica a la Dirección General de Recursos Humanos y Seguridad y a su jerarquía sobre cuestiones de seguridad relacionadas con su servicio y, de forma inmediata, sobre cualquier incidente relacionado con la seguridad, en particular aquellos en los que la ICUE o la información sensible no clasificada pueda haber quedado comprometida.
3. Para las cuestiones relacionadas con la seguridad de los sistemas de información y comunicación, el LSO se pondrá en contacto con el responsable local de seguridad informática (LISO) de su servicio de la Comisión, cuyas funciones y responsabilidades están establecidas en la Decisión C(2006) 3602.
4. El LSO contribuirá a las actividades de formación y sensibilización en materia de seguridad teniendo en cuenta las necesidades específicas del personal, los contratistas y otras personas que trabajen bajo la autoridad de su servicio.
5. Podrán asignarse al LSO tareas específicas en casos de riesgos graves o inmediatos para la seguridad, o en casos de emergencia, a petición de la Dirección General de Recursos Humanos y Seguridad. El director general o el director de Recursos Humanos de la Dirección General del LSO serán informados acerca de dichas tareas específicas por la Dirección General de Recursos Humanos y Seguridad.
6. Las responsabilidades del LSO se entenderán sin perjuicio de las funciones y responsabilidades asignadas a los responsables locales de seguridad informática (LISO), los responsables de salud y seguridad, los controladores del registro (RCO) o cualquier otra función que implique responsabilidades relacionadas con la seguridad o la protección. El LSO se pondrá en contacto con ellos a fin de garantizar un enfoque coherente y congruente de la seguridad y un flujo eficaz de información sobre cuestiones relacionadas con la seguridad en la Comisión.
7. El LSO tendrá acceso directo a su director general o jefe de servicio e informará a su jerarquía directa. Asimismo, deberá poseer una autorización de seguridad para acceder a ICUE, como mínimo hasta el nivel de SECRET UE/EU SECRET.
8. Con el fin de promover el intercambio de información y de mejores prácticas, la Dirección General de Recursos Humanos y Seguridad organizará al menos dos veces al año una conferencia de LSO. La presencia de los LSO en estas conferencias será obligatoria.

## CAPÍTULO 5

## APLICACIÓN

*Artículo 21***Normas de desarrollo y consignas de seguridad**

1. En caso necesario, la adopción de las normas de desarrollo de la presente Decisión será objeto de una decisión de habilitación distinta de la Comisión en favor del miembro de la Comisión responsable de las cuestiones de seguridad, de plena conformidad con el Reglamento interno.
2. Tras haber sido habilitado a raíz de la mencionada decisión de la Comisión, el miembro de la Comisión responsable de las cuestiones de seguridad podrá elaborar consignas de seguridad que establezcan directrices de seguridad y mejores prácticas, dentro del ámbito de aplicación de la presente Decisión y sus normas de desarrollo.
3. La Comisión podrá delegar las tareas mencionadas en los apartados 1 y 2 del presente artículo al director general de la Dirección General de Recursos Humanos y Seguridad mediante una decisión de delegación separada, de conformidad con el Reglamento interno.

## CAPÍTULO 6

**DISPOSICIONES VARIAS Y FINALES***Artículo 22***Tratamiento de datos personales**

1. La Comisión tratará los datos personales necesarios para la aplicación de la presente Decisión de conformidad con el Reglamento (CE) n° 45/2001.
2. Sin perjuicio de las medidas ya en vigor en el momento de la adopción de la presente Decisión y notificadas al Supervisor Europeo de Protección de Datos <sup>(1)</sup>, cualquier medida con arreglo a la presente Decisión que guarde relación con el tratamiento de datos personales, como las relativa a los registros de acceso y salida, grabaciones de circuito cerrado de televisión, grabaciones de llamadas telefónicas a servicios de permanencia o centros de expedición y datos similares, que sean necesarias por motivos de seguridad o de respuesta a las crisis, estarán sujetas a las normas de desarrollo de conformidad con lo dispuesto en el artículo 21, que establecerá las oportunas garantías para los interesados.
3. El director general de la Dirección General de Recursos Humanos y Seguridad será responsable de la seguridad del tratamiento de datos personales efectuado en el marco de la presente Decisión.
4. Las normas de desarrollo y los procedimientos se adoptarán previa consulta al responsable de la protección de datos y al Supervisor Europeo de Protección de Datos de conformidad con el Reglamento (CE) n° 45/2001.

*Artículo 23***Transparencia**

La presente Decisión y sus normas de desarrollo se pondrán en conocimiento del personal de la Comisión y de todas las personas a las que se aplican.

*Artículo 24***Derogación de decisiones anteriores**

Queda derogada la Decisión C(94) 2129.

*Artículo 25***Entrada en vigor**

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 13 de marzo de 2015.

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

---

<sup>(1)</sup> DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

**DECISIÓN (UE, Euratom) 2015/444 DE LA COMISIÓN**  
**de 13 de marzo de 2015**  
**sobre las normas de seguridad para la protección de la información clasificada de la UE**

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 249,

Visto el Tratado constitutivo de la Comunidad Europea de la Energía Atómica y, en particular, su artículo 106,

Visto el Protocolo nº 7 sobre los privilegios y las inmunidades de la Unión Europea anejo a los Tratados y, en particular, su artículo 18,

Considerando lo siguiente:

- (1) Las disposiciones de seguridad de la Comisión relativas a la protección de la información clasificada de la Unión Europea (ICUE) deben revisarse y actualizarse, teniendo en cuenta la evolución institucional, organizativa, operativa y tecnológica.
- (2) La Comisión Europea ha suscrito instrumentos sobre cuestiones de seguridad para sus sedes principales con los gobiernos de Bélgica, Luxemburgo e Italia <sup>(1)</sup>.
- (3) La Comisión, el Consejo y el Servicio Europeo de Acción Exterior se han comprometido a aplicar estándares de seguridad equivalentes para la protección de la ICUE.
- (4) Es importante que el Parlamento Europeo y las demás instituciones, órganos, organismos y agencias de la Unión queden asociados, cuando proceda, a los principios, estándares y normas de protección de la información clasificada que resultan necesarios para proteger los intereses de la Unión y de sus Estados miembros.
- (5) Los riesgos para la ICUE deberán gestionarse como un proceso. El objetivo de este proceso será determinar los riesgos conocidos para la seguridad, definir medidas de seguridad para reducir dichos riesgos a un nivel aceptable de conformidad con los principios básicos y normas mínimas establecidos en la presente Decisión, y aplicar estas medidas conforme al concepto de defensa en profundidad. La eficacia de dichas medidas será continuamente evaluada.
- (6) Dentro de la Comisión, por seguridad física dirigida a la protección de la información clasificada se entenderá la aplicación de medidas de protección físicas y técnicas para impedir el acceso no autorizado a la ICUE.
- (7) Por tratamiento de la ICUE se entenderá la aplicación de medidas administrativas de control de la ICUE a lo largo de todo su ciclo de vida que completen las medidas contempladas en los capítulos 2, 3 y 5 de la presente Decisión y contribuyan, así, a disuadir, descubrir y subsanar cualquier acto deliberado o accidental que pueda comprometer o suponer la pérdida de dicha información. Estas medidas se refieren, en particular, a la producción, almacenamiento, registro, copia, traducción, recalificación, desclasificación, traslado y destrucción de ICUE y complementan las normas generales sobre gestión de documentos de la Comisión [Decisiones 2002/47/CE, CECA, Euratom <sup>(2)</sup> y 2004/563/CE, Euratom <sup>(3)</sup>].

<sup>(1)</sup> Véase el «Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité» de 31 de diciembre de 2004, el «Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois», de 20 de enero de 2007, y el «Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale», de 22 de julio de 1959.

<sup>(2)</sup> Decisión 2002/47/CE, CECA, Euratom de la Comisión, de 23 de enero de 2002, por la que se modifica su Reglamento interno (DO L 21 de 24.1.2002, p. 23).

<sup>(3)</sup> Decisión 2004/563/CE, Euratom de la Comisión, de 7 de julio de 2004, por la que se modifica su Reglamento interno (DO L 251 de 27.7.2004, p. 9).

- (8) Las disposiciones de la presente Directiva no afectarán a:
- Reglamento (Euratom) n° 3 <sup>(1)</sup>;
  - Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo <sup>(2)</sup>;
  - Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo <sup>(3)</sup>;
  - Reglamento (CEE, Euratom) n° 354/83 del Consejo <sup>(4)</sup>.

HA ADOPTADO LA PRESENTE DECISIÓN:

#### CAPÍTULO 1

### PRINCIPIOS BÁSICOS Y ESTÁNDARES MÍNIMOS

#### Artículo 1

#### Definiciones

A efectos de la presente Decisión, se entenderá por:

- «Servicio de la Comisión»: toda Dirección General o servicio de la Comisión, o cualquier gabinete de un miembro de la Comisión.
- «Material de cifra»: algoritmos criptológicos, módulos criptológicos de software y hardware, y productos, incluida la información sobre su uso y la documentación pertinente y los datos de claves.
- «Desclasificación»: supresión de toda clasificación de seguridad.
- «Defensa en profundidad»: aplicación de una serie de medidas de seguridad organizadas a modo de defensa en barreras sucesivas.
- «Documento»: toda información registrada, independientemente de su soporte o características físicas.
- «Reducción del grado de clasificación»: reducción del grado de clasificación de seguridad.
- «Manejo» de ICUE: toda intervención posible a la que puede estar sujeta a lo largo de su ciclo de vida la ICUE, es decir: producción, registro, tratamiento, traslado, reducción del grado de clasificación, desclasificación y destrucción. En relación con los sistemas de información y comunicaciones (SIC) abarca asimismo su recopilación, exposición, transmisión y almacenamiento.
- «Poseedor»: persona debidamente autorizada con una probada necesidad de conocer la información, que está en posesión de cualquier ICUE y es, por tanto, responsable de su protección.
- «Normas de desarrollo»: todo conjunto de normas o directrices de seguridad adoptado de conformidad con el capítulo 5 de la Decisión (EU, Euratom) 2015/443 de la Comisión <sup>(5)</sup>.
- «Material»: todo medio, soporte de datos, máquina o aparato, producido o en proceso de producción.
- «Originador»: institución, organismo o agencia de la Unión, Estado miembro, tercer Estado u organización internacional bajo cuya autoridad se ha producido información clasificada o se ha introducido en las estructuras de la Unión.
- «Locales»: todo inmueble o propiedad y posesiones asimiladas de la Comisión.

<sup>(1)</sup> Reglamento (Euratom) n° 3, de 31 de julio de 1958, relativo a la aplicación del artículo 24 del Tratado constitutivo de la Comunidad Europea de la Energía Atómica (DO L 17 de 6.10.1958, p. 406/58).

<sup>(2)</sup> Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

<sup>(3)</sup> Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

<sup>(4)</sup> Reglamento (CEE, Euratom, CECA) n° 354/83 del Consejo, de 1 de febrero de 1983, relativo a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía Atómica (DO L 43 de 15.2.1983, p. 1).

<sup>(5)</sup> Decisión (UE, Euratom) 2015/443 de la Comisión, de 13 de marzo de 2015, sobre la seguridad en la Comisión (véase la página 41 del presente Diario Oficial).



- 13) «Proceso de gestión de riesgos de seguridad»: totalidad del proceso de determinación, control y disminución de acontecimientos inciertos que puedan afectar a la seguridad de una organización o de cualquiera de los sistemas que utiliza. Abarca todas las actividades relacionadas con los riesgos, incluida la evaluación, tratamiento, aceptación y comunicación.
- 14) «Estatuto de los funcionarios»: Estatuto de los funcionarios de la Unión Europea y Régimen aplicable a otros agentes de la Unión Europea establecido mediante el Reglamento (CEE, Euratom, CECA) n° 259/68 del Consejo <sup>(1)</sup>.
- 15) «Amenaza»: posible causa de un incidente no deseado que pueda ocasionar daños a una organización o a algunos de los sistemas que use; las amenazas pueden ser accidentales o deliberadas (maliciosas) y constan de elementos amenazadores, posibles blancos y métodos de ataque.
- 16) «Vulnerabilidad»: debilidad, cualquiera que sea su naturaleza, que pueda ser aprovechada por una o varias amenazas. La vulnerabilidad puede resultar de una omisión o guardar relación con una deficiencia en el grado, completitud o coherencia de los controles, y puede ser técnica, física, de procedimiento, de organización o de funcionamiento.

#### Artículo 2

### Objeto y ámbito de aplicación

1. La presente Decisión establece los principios básicos y los estándares mínimos de seguridad para la protección de la información clasificada de la Unión Europea (ICUE).
2. La presente Decisión se aplicará a todos los servicios de la Comisión y en todos los locales de la Comisión.
3. Sin perjuicio de las indicaciones específicas relativas a grupos concretos de personal, la presente Decisión se aplicará a los miembros de la Comisión, al personal de la Comisión incluido en el ámbito de aplicación del Estatuto de los funcionarios y de las condiciones de empleo de otros agentes de las Comunidades Europeas, a los expertos nacionales enviados en comisión de servicio a la Comisión (en lo sucesivo, «expertos nacionales en comisión de servicios»), a los proveedores de servicios y su personal, a los trabajadores en prácticas y a cualquier persona con acceso a los edificios de la Comisión u otros activos, o a la información manejada por la Comisión.
4. Las disposiciones de la presente Decisión se entenderán sin perjuicio de lo dispuesto en la Decisión 2002/47/CE, CECA, Euratom y la Decisión 2004/563/CE, Euratom.

#### Artículo 3

### Definición de ICUE, clasificaciones de seguridad y marcas

1. Por «información clasificada de la UE» (ICUE) se entenderá toda información o material a los que se haya asignado una clasificación de seguridad de la UE cuya revelación no autorizada pueda causar perjuicio en distintos grados a los intereses de la Unión Europea o de uno o varios Estados miembros.
2. La ICUE se clasificará en uno de los grados siguientes:
  - a) TRES SECRET UE/EU TOP SECRET: información y material cuya revelación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros;
  - b) SECRET UE/EU SECRET: información y material cuya revelación no autorizada pueda causar un perjuicio grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros;
  - c) CONFIDENTIEL UE/EU CONFIDENTIAL: información y material cuya revelación no autorizada pueda causar perjuicio a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros;
  - d) RESTREINT UE/EU RESTRICTED: información y material cuya revelación no autorizada pueda resultar desfavorable para los intereses de la Unión Europea o de uno o varios Estados miembros.
3. La ICUE llevará una marca de clasificación de seguridad de conformidad con el apartado 2. Podrá llevar marcas suplementarias que no sean marcas de clasificación, sino que se destinen a designar el ámbito de actividad al que se refiere, identificar el originador, limitar la difusión, restringir su utilización o indicar la medida en que puede ser cedida.

<sup>(1)</sup> Reglamento (CEE, Euratom, CECA) n° 259/68 del Consejo, de 29 de febrero de 1968, por el que se establece el Estatuto de los funcionarios de las Comunidades Europeas y el régimen aplicable a los otros agentes de estas Comunidades y por el que se establecen medidas específicas aplicables temporalmente a los funcionarios de la Comisión (DO L 56 de 4.3.1968, p. 1).

*Artículo 4***Gestión de la clasificación**

1. Cada uno de los miembros de la Comisión o de los servicios de la Comisión se asegurarán de que la ICUE que crean se clasifique adecuadamente, quede claramente marcada como ICUE y solo conserve su grado de clasificación mientras sea necesario.
2. Sin perjuicio de lo dispuesto en el artículo 26, no se podrá rebajar el grado de clasificación de la ICUE ni desclasificarla, ni modificar o suprimir las marcas de clasificación de seguridad a que se refiere el artículo 3, apartado 2, sin el consentimiento previo por escrito del originador.
3. En su caso, se adoptarán normas de desarrollo para el manejo de la ICUE, que incluirán una guía práctica de clasificación, de conformidad con el artículo 60.

*Artículo 5***Protección de la información clasificada**

1. La ICUE se protegerá de conformidad con la presente Decisión y sus normas de desarrollo.
2. El poseedor de cualquier ICUE tendrá la responsabilidad de protegerla de conformidad con la presente Decisión y sus normas de desarrollo, con arreglo a las normas previstas en el capítulo 4.
3. Cuando los Estados miembros introduzcan en las estructuras o redes de la Comisión información clasificada que lleve una marca nacional de clasificación de seguridad, la Comisión protegerá dicha información con arreglo a los requisitos aplicables a la ICUE del grado equivalente, según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el anexo I.
4. Un agregado de ICUE podrá justificar un grado de protección que corresponda a una clasificación más elevada que la asignada a cada uno de sus componentes.

*Artículo 6***Gestión del riesgo de seguridad**

1. Las medidas de seguridad para proteger la ICUE a lo largo de todo su ciclo de vida serán acordes, en particular, con su clasificación de seguridad, la forma y el volumen de la información o material, la ubicación y construcción de la instalación en la que se conserve, y la amenaza de actividades maliciosas o delictivas, evaluadas localmente, en particular el espionaje, el sabotaje y el terrorismo.
2. Los planes de contingencia tendrán en cuenta la necesidad de proteger la ICUE en situaciones de emergencia, con el fin de impedir el acceso o la revelación no autorizados y la pérdida de integridad o disponibilidad.
3. En los planes de continuidad de la actividad de todos los servicios se incluirán medidas preventivas y de recuperación para reducir al máximo las repercusiones de fallos o incidentes graves en el manejo y almacenamiento de la ICUE.

*Artículo 7***Aplicación de la presente Decisión**

1. En caso necesario, se adoptarán normas de desarrollo que completen o faciliten la aplicación de la presente Decisión, con arreglo a lo dispuesto en el artículo 60.
2. Los servicios de la Comisión adoptarán todas las medidas necesarias que sean de su competencia con el fin de garantizar que, cuando manejen o almacenen ICUE o cualquier otra información clasificada, se apliquen la presente Decisión y las normas de desarrollo correspondientes.
3. Las medidas de seguridad adoptadas en aplicación de la presente Decisión deberán ajustarse a los principios de seguridad de la Comisión establecidos en el artículo 3 de la Decisión (UE, Euratom) 2015/443.

4. El director general de la Dirección General de Recursos Humanos y Seguridad establecerá la autoridad de seguridad de la Comisión en el seno de la Dirección General de Recursos Humanos y Seguridad. La autoridad de seguridad de la Comisión dispondrá de las competencias que le sean asignadas por la presente Decisión y sus normas de desarrollo.
5. En cada servicio de la Comisión, el responsable local de Seguridad (LSO), tal como se contempla en el artículo 20 de la Decisión (UE, Euratom) 2015/443, tendrá las siguientes responsabilidades generales en materia de protección de la ICUE conforme a lo dispuesto en la presente Decisión, en estrecha cooperación con la Dirección General de Recursos Humanos y Seguridad:
  - a) gestión de las solicitudes de autorizaciones de seguridad para el personal;
  - b) contribución a la formación en materia de seguridad y sesiones de información sobre sensibilización;
  - c) supervisión del controlador del registro (RCO) del servicio;
  - d) información sobre fallos de seguridad y comprometimiento de la ICUE;
  - e) custodia de llaves de repuesto y registro escrito de cada combinación;
  - f) asunción de otras tareas relacionadas con la protección de la ICUE o establecidas por las normas de desarrollo.

#### Artículo 8

##### **Fallos de seguridad y comprometimiento de la ICUE**

1. Un fallo de seguridad se produce como resultado de una acción u omisión de una persona contraria a las normas de seguridad establecidas en la presente Decisión y sus normas de desarrollo.
2. Se produce un comprometimiento de la ICUE cuando, como consecuencia de un fallo de seguridad, dicha información se pone total o parcialmente en conocimiento de personas no autorizadas.
3. Todo fallo o posible fallo de seguridad deberá comunicarse inmediatamente a la autoridad de seguridad de la Comisión.
4. Cuando se tenga conocimiento o sospechas fundadas de que una ICUE se ha visto comprometida o se ha perdido, se realizará una investigación de seguridad con arreglo a lo dispuesto en el artículo 13 de la Decisión (UE, Euratom) 2015/443.
5. Se tomarán todas las medidas adecuadas para:
  - a) informar al originador de la información;
  - b) asegurarse de que el personal que investiga el caso con el fin de esclarecer los hechos no esté directamente implicado en el fallo de seguridad;
  - c) evaluar el posible perjuicio causado a los intereses de la Unión o de los Estados miembros;
  - d) tomar medidas adecuadas a fin de impedir que se repitan esos hechos; y
  - e) notificar a las autoridades que corresponda las medidas adoptadas.
6. La persona que sea responsable de un fallo de las normas de seguridad establecidas en la presente Decisión podrá ser objeto de medidas disciplinarias de conformidad con el Estatuto de los funcionarios. La persona que sea responsable de un comprometimiento o pérdida de ICUE podrá ser objeto de medidas disciplinarias o de una acción judicial de conformidad con las disposiciones legales y reglamentarias aplicables.

#### CAPÍTULO 2

##### **SEGURIDAD EN EL PERSONAL**

#### Artículo 9

##### **Definiciones**

A los efectos del presente capítulo, se entenderá por:

- 1) «Autorización para acceder a ICUE»: decisión de la autoridad de seguridad de la Comisión, adoptada sobre la base de una garantía concedida por una autoridad competente de un Estado miembro, que acredita que un funcionario u otro agente de la Comisión o experto nacional destinado en la Comisión en comisión de servicio puede tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada, siempre que se haya establecido su necesidad de conocer dicha información y haya sido adecuadamente informado sobre sus responsabilidades. De la persona que se ajuste a esta descripción se dirá que tiene «autorización de seguridad».

- 2) «Autorización personal de seguridad»: aplicación de medidas que garanticen que el acceso a la ICUE se concede únicamente a personas que:
  - a) tengan necesidad de conocer;
  - b) hayan sido habilitadas para el grado de clasificación correspondiente, en caso necesario, y
  - c) hayan sido instruidas sobre sus responsabilidades.
- 3) «Habilitación personal de seguridad» (HPS): declaración de una autoridad competente de un Estado miembro, efectuada al término de una investigación de seguridad realizada por las autoridades competentes del Estado miembro, mediante la cual se acredita que una persona puede, siempre que se haya determinado su «necesidad de conocer» y haya sido adecuadamente informada de sus responsabilidades, tener acceso a ICUE de un determinado grado (CONFIDENTIEL UE/EU CONFIDENTIAL o superior) hasta una fecha determinada.
- 4) «Certificado de habilitación personal de seguridad» (CHPS): certificado expedido por una autoridad competente mediante el cual se establece que una persona dispone de un certificado de habilitación de seguridad o una autorización válidos para acceder a ICUE expedidos por la autoridad de seguridad de la Comisión, y que indica el grado de ICUE a que puede tener acceso (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), el período de validez de la habilitación y la fecha de caducidad del propio certificado.
- 5) «Investigación de seguridad»: procedimiento de investigación efectuado por la autoridad competente de un Estado miembro con arreglo a las disposiciones legales y reglamentarias nacionales vigentes, con el fin de obtener la garantía de que no se conocen datos desfavorables que impidan conceder a una persona determinada una habilitación de seguridad para acceder a ICUE de un determinado nivel (CONFIDENTIEL UE/EU CONFIDENTIAL o superior).

#### Artículo 10

#### Principios básicos

1. Solo se concederá acceso a ICUE a aquella persona:
  - 1) cuya necesidad de conocer se haya determinado;
  - 2) que haya sido instruida sobre las normas de seguridad para la protección de la ICUE y las correspondientes directrices y estándares de seguridad, y que haya aceptado sus responsabilidades en lo que respecta a la protección de dicha información;
  - 3) en el caso de información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior: a quien se haya concedido una habilitación en el grado correspondiente, o bien a quien se haya autorizado debidamente en virtud de sus funciones, de conformidad con las disposiciones legales y reglamentarias nacionales.
2. Todas las personas cuyas funciones puedan requerir el acceso a ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior deberán haber sido habilitadas para el grado correspondiente antes de poder acceder a dicha información. La persona de que se trate dará su consentimiento por escrito para ser sometida al procedimiento de habilitación de seguridad. De no hacerlo, se entenderá que el interesado no puede ser destinado a un puesto de trabajo, función o misión que implique el acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior.
3. Los procedimientos de habilitación personal de seguridad estarán concebidos para determinar si una persona puede ser autorizada para acceder a la ICUE, teniendo en cuenta su lealtad, honradez y fiabilidad.
4. La lealtad, honradez y fiabilidad de una persona a efectos de la obtención de una habilitación de seguridad para acceder a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se determinarán mediante una investigación de seguridad realizada por las autoridades competentes de un Estado miembro, de conformidad con sus disposiciones legales y reglamentarias nacionales.
5. La autoridad de seguridad de la Comisión será la única responsable de la coordinación con las autoridades nacionales de seguridad (ANS) u otras autoridades nacionales competentes en el contexto de todas las cuestiones relacionadas con la habilitación de seguridad. Todos los contactos entre los servicios de la Comisión y su personal y las ANS y otras autoridades competentes se efectuarán a través de la autoridad de seguridad de la Comisión.

#### Artículo 11

#### Procedimiento de autorización de seguridad

1. Cada director general o jefe de servicio de la Comisión determinará los puestos dentro de sus servicios cuyos titulares deben tener acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior para cumplir sus obligaciones en materia de seguridad y deben, por tanto, ser autorizados.

2. En cuanto tenga conocimiento de que una persona será nombrada para un puesto que requiera acceso a información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, el LSO del servicio de la Comisión de que se trate informará a la autoridad de seguridad de la Comisión, que remitirá a la persona el cuestionario de habilitación de seguridad emitido por la ANS del Estado miembro en virtud de cuya nacionalidad la persona haya sido nombrada miembro del personal de las instituciones europeas. El interesado deberá dar su consentimiento por escrito para ser sometido al procedimiento de habilitación de seguridad y enviará el cuestionario debidamente cumplimentado en el plazo más breve a la autoridad de seguridad de la Comisión.
3. La autoridad de seguridad de la Comisión remitirá el cuestionario de habilitación de seguridad cumplimentado a la ANS del Estado miembro en virtud de cuya nacionalidad la persona haya sido nombrada miembro del personal de las instituciones europeas, solicitando que se lleve a cabo una investigación de seguridad para el nivel de la ICUE a que el interesado requerirá acceso.
4. En los casos en que la autoridad de seguridad de la Comisión tenga información pertinente para una investigación de seguridad sobre una persona que ha solicitado una habilitación de seguridad, la autoridad de seguridad de la Comisión, con arreglo a las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS competente.
5. Una vez concluida la investigación de seguridad, y tan pronto como sea posible después de haber sido notificada por la ANS pertinente acerca de su evaluación general de las conclusiones de dicha investigación, la autoridad de seguridad de la Comisión:
  - a) podrá conceder una autorización de acceso a la ICUE a la persona de que se trate y autorizar el acceso a la ICUE del grado pertinente hasta una fecha que especifique, pero para un período máximo de 5 años, en caso de que la investigación de seguridad permita garantizar que no se conoce ningún dato desfavorable que ponga en entredicho la lealtad, honradez y fiabilidad de la persona;
  - b) en caso de que la investigación de seguridad no permita dar semejante garantía, de conformidad con las disposiciones legales y reglamentarias pertinentes, lo notificará a la persona, que podrá requerir ser oída por la autoridad de seguridad de la Comisión, quien, a su vez, podrá pedir a la ANS competente cuantas aclaraciones le pueda facilitar, de conformidad con sus disposiciones legales y reglamentarias nacionales. En caso de que el resultado de la investigación de seguridad se confirme, no se expedirá la autorización de acceso a la ICUE.
6. La investigación de seguridad, junto con los resultados obtenidos deberá ser conforme a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión, incluido todo lo relativo a recursos. Se podrá apelar contra las decisiones de la autoridad de seguridad de la Comisión de acuerdo con lo dispuesto en el Estatuto de los funcionarios.
7. La Comisión aceptará la autorización de acceso a ICUE concedida por otra institución, órgano u organismo de la Unión, siempre que siga siendo válida. La autorización valdrá para cualquier nombramiento de la persona en la Comisión. La institución, órgano u organismo de la Unión que contrate a la persona notificará a la ANS correspondiente el cambio de empleador.
8. En caso de que el período de servicio de la persona no haya comenzado al término de 12 meses a partir de la notificación del resultado de la investigación de seguridad a la autoridad de seguridad de la Comisión, o en caso de que haya una interrupción de 12 meses en el tiempo de servicio de esa misma persona durante el cual no haya estado empleada en la Comisión ni en otra institución, órgano u organismo de la Unión, ni en una administración nacional de un Estado miembro, la autoridad de seguridad de la Comisión remitirá el asunto a la ANS correspondiente para que confirme que sigue siendo válido y adecuado.
9. Si la autoridad de seguridad de la Comisión tuviera conocimiento de que una persona que tiene autorización para acceder a ICUE representa un riesgo para la seguridad, la autoridad de seguridad de la Comisión, con arreglo a las disposiciones legales y reglamentarias pertinentes, lo notificará a la ANS correspondiente.
10. Si una ANS notifica a la autoridad de seguridad de la Comisión la retirada de una garantía concedida de conformidad con el apartado 5, letra a), a una persona que tiene autorización de acceso a ICUE, la autoridad de seguridad de la Comisión podrá pedir a la ANS cuantas aclaraciones pueda facilitar, de conformidad con sus disposiciones legales y reglamentarias nacionales. Si se confirma la información desfavorable, se le retirará la autorización y se le excluirá del acceso a ICUE y de los puestos en los que pudiera tener acceso a dicha información o poner en peligro la seguridad.
11. La decisión de retirar o suspender una autorización de acceso a ICUE a una persona que entre en el ámbito de aplicación de la presente Decisión, y, en su caso, los motivos para hacerlo, se comunicarán a la persona, que podrá requerir ser oída por la autoridad de seguridad de la Comisión. La información facilitada por la ANS deberá ajustarse a las disposiciones legales y reglamentarias vigentes en el Estado miembro en cuestión. Se podrá apelar contra las decisiones de la autoridad de seguridad de la Comisión de acuerdo con lo dispuesto en el Estatuto de los funcionarios.

12. Los servicios de la Comisión deberán asegurarse de que los expertos nacionales en comisión de servicio para un puesto que requiera autorización de seguridad para acceder a ICUE presenten, antes de asumir sus funciones, una HPS o un Certificado de Habilitación Personal de Seguridad (CHPS) válidos, de conformidad con la normativa y la legislación nacional, a la autoridad de seguridad de la Comisión que, basándose en ello, expedirá una autorización para acceder a ICUE hasta el nivel equivalente a aquel a que se refiere la habilitación nacional de seguridad, con una validez máxima igual al período de la misión.

#### Acceso a ICUE de personas debidamente autorizadas en virtud de sus funciones

13. Los miembros de la Comisión, que tengan acceso a ICUE en virtud de sus funciones sobre la base del Tratado, serán informados de sus obligaciones respecto de la protección de la ICUE.

#### Habilitaciones de seguridad y registros de la autorización de seguridad

14. La autoridad de seguridad de la Comisión conservará registros de las habilitaciones de seguridad y de las autorizaciones concedidas para acceder a ICUE, de conformidad con lo dispuesto en la presente Decisión. Estos registros indicarán, como mínimo, el nivel de ICUE al que el interesado puede tener acceso, la fecha de concesión de la habilitación de seguridad y su período de validez.

15. La autoridad de seguridad de la Comisión podrá expedir un CHPS que acredite a qué grado de ICUE puede tener acceso la persona (CONFIDENTIEL UE/EU CONFIDENTIAL o superior), la fecha de validez de la autorización para acceder a la ICUE de que se trate y la fecha de caducidad del propio certificado.

#### Renovación de las autorizaciones de seguridad

16. Tras la concesión inicial de una autorización de seguridad, y siempre que la persona haya prestado servicio de forma ininterrumpida en la Comisión Europea u otra institución, órgano u organismo de la Unión y siga necesitando acceder a ICUE, la autorización de seguridad se revisará con vistas a su renovación, con carácter general, cada 5 años a partir de la fecha de notificación del resultado de la última investigación de seguridad que haya servido de base para dicha autorización.

17. La autoridad de seguridad de la Comisión podrá prorrogar la validez de la autorización de seguridad vigente por un período de hasta 12 meses, si no se ha recibido información desfavorable de la ANS pertinente o de otra autoridad nacional competente en un plazo de 2 meses a partir de la fecha de envío de la solicitud de renovación y del correspondiente cuestionario de habilitación de seguridad. Si al término de este período de 12 meses, la ANS pertinente u otro organismo nacional competente no ha comunicado a la autoridad de seguridad de la Comisión su dictamen, la persona solo podrá desempeñar funciones que no requieran una habilitación de seguridad.

### *Artículo 12*

#### **Sesiones informativas en materia de autorización de seguridad**

1. Tras participar en la sesión informativa en materia de autorización de seguridad organizada por la autoridad de seguridad de la Comisión, todas las personas que hayan recibido una autorización de seguridad reconocerán por escrito que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias del comprometimiento de esta información. La autoridad de seguridad de la Comisión llevará un registro de estas declaraciones escritas.

2. Desde un principio, se sensibilizará a todas las personas que estén autorizadas para acceder a ICUE o que deban manejar este tipo de información, respecto de las amenazas a la seguridad, sobre las que se les aleccionará periódicamente. Dichas personas deberán dar cuenta inmediatamente a la autoridad de seguridad de la Comisión de cualquier actitud o actividad que consideren sospechosa o inusual.

3. Todas las personas que dejen de desempeñar funciones que requieran el acceso a ICUE serán aleccionadas sobre su obligación de seguir protegiendo dicha información, y, en su caso, deberán reconocer tal obligación por escrito.

### *Artículo 13*

#### **Autorizaciones de seguridad temporales**

1. En circunstancias excepcionales, cuando esté debidamente justificado en interés del servicio y en espera de la conclusión de una investigación de seguridad completa, la autoridad de seguridad de la Comisión podrá conceder una autorización temporal para acceder a ICUE para una función específica, tras haber consultado a la ANS del Estado miembro del que sea nacional la persona y con supeditación al resultado de las indagaciones preliminares encaminadas a verificar que no se conoce ninguna información desfavorable de la misma, sin perjuicio de las disposiciones relativas a la renovación de las habilitaciones de seguridad. La validez de estas autorizaciones temporales no será superior a 6 meses ni permitirá acceder a información clasificada de grado TRÈS SECRET UE/EU TOP SECRET.

2. Tras haber sido informadas de conformidad con el artículo 12, apartado 1, todas las personas a las que se haya concedido una autorización temporal reconocerán en una declaración escrita que han entendido sus obligaciones respecto a la protección de la ICUE y las consecuencias del comprometimiento de esta información. La autoridad de seguridad de la Comisión llevará un registro de estas declaraciones escritas.

#### Artículo 14

##### **Asistencia a reuniones clasificadas organizadas por la Comisión**

1. Los servicios de la Comisión responsables de la organización de reuniones en las que se examinará información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior, a través de su LSO o a través del organizador de la reunión, informarán a la autoridad de seguridad de la Comisión con mucha antelación de las fechas, horarios, lugar y participantes en dichas reuniones.
2. Sin perjuicio de las disposiciones del artículo 11, apartado 13, las personas que deban participar en reuniones organizadas por la Comisión en las que se examine información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior solo podrán hacerlo previa comprobación de la situación de su habilitación de seguridad o autorización de seguridad. Se denegará el acceso a este tipo de reuniones confidenciales a las personas para las que la autoridad de seguridad de la Comisión no haya comprobado la existencia de un CHSP u otra prueba de habilitación de seguridad, o a participantes de la Comisión que no posean una autorización de seguridad.
3. Antes de organizar una reunión clasificada, el organizador de la reunión o el LSO del servicio de la Comisión que haya organizado la reunión solicitará a los participantes externos que proporcionen a la autoridad de seguridad de la Comisión un CHSP u otra prueba de habilitación de seguridad. La autoridad de seguridad de la Comisión informará al LSO o al organizador de la reunión acerca de los CHSP u otra prueba de HPS recibidos. Cuando proceda, podrá utilizarse una lista recapitulativa de nombres en la que figuren las pruebas pertinentes de su habilitación de seguridad.
4. En caso de que la autoridad de seguridad de la Comisión sea informada por las autoridades competentes de que se ha retirado la HPS a una persona cuyas funciones requieran la asistencia a reuniones organizadas por la Comisión, la autoridad de seguridad de la Comisión deberá informar de inmediato al LSO del servicio de la Comisión responsable de la organización de la reunión.

#### Artículo 15

##### **Acceso potencial a ICUE**

Los correos, agentes de seguridad y escoltas serán debidamente autorizados para el grado correspondiente o investigados de forma apropiada según las disposiciones legales y reglamentarias nacionales, se les aleccionará sobre los procedimientos de seguridad para la protección de la ICUE y se les instruirá acerca de sus obligaciones en materia de protección de la información que se les confíe.

#### CAPÍTULO 3

##### **SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA**

#### Artículo 16

##### **Principios básicos**

1. Las medidas de seguridad física estarán concebidas para impedir la entrada, subrepticia o por la fuerza, de intrusos, para disuadir, impedir y descubrir actividades no autorizadas y para segregar al personal en lo que respecta al acceso a ICUE según el principio de necesidad de conocer el contenido de dicha información. Estas medidas se determinarán a partir de un proceso de gestión de riesgos, de conformidad con la presente Decisión y sus normas de desarrollo.
2. Las medidas de seguridad física estarán concebidas para impedir el acceso no autorizado a ICUE, en particular:
  - a) garantizando que la ICUE se maneje y almacene adecuadamente;
  - b) permitiendo la separación del personal en cuanto a su acceso a ICUE en función de su necesidad de conocer y, en su caso, de su autorización de seguridad;
  - c) disuadiendo, impidiendo y detectando actividades no autorizadas, e
  - d) impidiendo o retrasando la entrada subrepticia o por la fuerza de intrusos.

3. Se establecerán medidas de seguridad física en todos los locales, edificios, oficinas, salas y demás zonas en que se maneje o almacene ICUE, incluidas las zonas que alberguen sistemas de información y comunicaciones, en el sentido definido en el capítulo 5.
4. Las zonas en que se almacene ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se establecerán como Zonas de Acceso Restringido, de conformidad con el presente capítulo, y serán aprobadas por la autoridad de seguridad de la Comisión.
5. Para la protección de ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior solo podrán emplearse equipos o dispositivos aprobados por la autoridad de seguridad de la Comisión.

#### Artículo 17

##### Requisitos y medidas de seguridad física

1. Las medidas de seguridad física aplicables se determinarán sobre la base de una evaluación de las amenazas realizada por la autoridad de seguridad de la Comisión, si procede en consulta con otros servicios de la Comisión, otras instituciones, órganos u organismos de la Unión o autoridades competentes de los Estados miembros. La Comisión aplicará un proceso de gestión de riesgos para proteger la ICUE en sus locales, de modo que se garantice un grado de protección física acorde con el riesgo evaluado. El proceso de gestión de riesgos tendrá en cuenta todos los factores pertinentes, en particular:
  - a) el grado de clasificación de la ICUE;
  - b) la forma y volumen de la ICUE, teniendo presente que grandes cantidades de ICUE o su recopilación podrían requerir la aplicación de medidas de protección más estrictas;
  - c) el entorno y la estructura de los edificios o zonas donde se guarde ICUE, y
  - d) la evaluación de las amenazas que representan tanto los servicios de inteligencia que tienen como objetivo la Unión y sus instituciones, órganos u organismos, o los Estados miembros, como el sabotaje, el terrorismo, la subversión u otras actividades delictivas.
2. Al aplicar el concepto de defensa en profundidad, la autoridad de seguridad de la Comisión determinará la combinación apropiada de las medidas de seguridad física que deben aplicarse. A tal efecto, elaborará estándares, normas y criterios mínimos establecidos en las normas de desarrollo.
3. Podrá autorizarse a la autoridad de seguridad de la Comisión a llevar a cabo, en las entradas y salidas, registros que disuadan de todo intento no autorizado de introducir material en los locales o edificios o de sacar de ellos ICUE.
4. Cuando exista el riesgo de que una ICUE sea objeto de miradas indiscretas, incluso accidentalmente, los servicios de la Comisión tomarán medidas adecuadas, definidas por la autoridad de seguridad de la Comisión, para contrarrestar ese riesgo.
5. Para los nuevos establecimientos, los requisitos de seguridad física y sus especificaciones funcionales se definirán de acuerdo con la autoridad de seguridad de la Comisión como parte de la planificación y el diseño de los mismos. Para los establecimientos ya existentes, los requisitos de seguridad física se aplicarán de conformidad con los estándares, normas y criterios mínimos establecidos en las normas de desarrollo.

#### Artículo 18

##### Equipo para la protección física de la ICUE

1. Para la protección física de la ICUE se establecerán dos tipos de zonas físicamente protegidas:
  - a) zonas administrativas, y
  - b) zonas de acceso restringido (incluidas las zonas de acceso restringido protegidas por medios técnicos).
2. La Autoridad de Acreditación de Seguridad de la Comisión decidirá si una zona cumple los requisitos para ser designada zona administrativa, zona de acceso restringido o zona de acceso restringido protegida por medios técnicos.
3. Para las zonas administrativas:
  - a) se establecerá un perímetro visiblemente definido que permita el control de las personas y, cuando sea posible, de los vehículos;
  - b) solo se permitirá el acceso sin acompañamiento a las personas debidamente autorizadas por la autoridad de seguridad de la Comisión o cualquier otra autoridad competente, y
  - c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.



4. Para las zonas de acceso restringido:
  - a) se establecerá un perímetro visiblemente definido y protegido en el que se controlen todas las entradas y salidas mediante un sistema de pases o de identificación personal;
  - b) solo se permitirá el acceso sin acompañamiento a las personas que tengan una habilitación de seguridad y una autorización específica para entrar en la zona por su necesidad de conocer;
  - c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.
5. Cuando la entrada en una zona de acceso restringido equivalga en la práctica a tener acceso directo a la información clasificada que se encuentre en la zona, se aplicarán además los siguientes requisitos:
  - a) se indicará con claridad el máximo grado de clasificación de seguridad de la información que se encuentre normalmente en dicha zona;
  - b) todos los visitantes necesitarán una autorización específica para acceder a la zona, estarán acompañados en todo momento y debidamente habilitados, salvo que se tomen medidas para que no sea posible que accedan a la ICUE.
6. Las zonas de acceso restringido protegidas contra escuchas serán designadas como zonas de acceso restringido protegidas por medios técnicos. Se aplicarán los requisitos adicionales siguientes:
  - a) estas zonas estarán equipadas con sistemas de detección de intrusos («SDI»), se cerrarán con llave cuando no estén ocupadas y se vigilarán cuando estén ocupadas; todas las llaves se controlarán de acuerdo con lo dispuesto en el artículo 20;
  - b) todas las personas y el material que entren en estas zonas serán objeto de control;
  - c) estas zonas serán objeto de inspecciones físicas o técnicas regularmente por la autoridad de seguridad de la Comisión; además, serán inspeccionadas también cada vez que se haya producido o se sospeche que se ha producido una entrada no autorizada, y
  - d) no habrá en estas zonas ninguna línea de comunicaciones, teléfono ni otro equipo de comunicaciones, ni aparatos eléctricos o electrónicos, salvo los que estén autorizados.
7. No obstante lo dispuesto en el punto 6, letra d), todos los equipos de comunicaciones y todos los aparatos eléctricos o electrónicos deberán ser examinados por la autoridad de seguridad de la Comisión antes de que puedan ser utilizados en zonas donde se estén celebrando reuniones o realizando trabajos en que se maneje información clasificada de grado SECRET UE/EU SECRET y superior, y cuando la amenaza para la ICUE se considere elevada, con el fin de garantizar que ninguna información en claro pueda transmitirse de manera involuntaria o ilícita a través de dichos equipos más allá del perímetro de la zona de acceso restringido de que se trate.
8. Las zonas de acceso restringido que no estén ocupadas por personal de servicio las 24 horas del día se inspeccionarán, en su caso, al final de la jornada normal de trabajo y a intervalos aleatorios fuera de dicha jornada, a menos que se haya instalado en ellas un sistema de detección de intrusos.
9. Se podrán establecer con carácter temporal zonas de acceso restringido y zonas de acceso restringido protegidas por medios técnicos en una zona administrativa para la celebración de una reunión clasificada u otro motivo similar.
10. El LSO del servicio de la Comisión de que se trate definirá procedimientos operativos de seguridad para cada zona de acceso restringido bajo su responsabilidad en los que se disponga lo siguiente, de conformidad con las disposiciones de la presente Decisión y de sus normas de desarrollo:
  - a) el grado de la ICUE que puede manejarse o almacenarse en la zona;
  - b) las medidas de vigilancia y protección que hayan de aplicarse;
  - c) las personas autorizadas para entrar en ella sin acompañamiento en virtud de su necesidad de conocer y de su autorización de seguridad;
  - d) si ha lugar, los procedimientos aplicables a los acompañantes o a la protección de la ICUE cuando se autorice la entrada de cualquier otra persona en la zona;
  - e) cualquier otra medida o procedimiento pertinente.
11. Las cámaras acorazadas se ubicarán en zonas de acceso restringido. Los muros, suelos, techos, ventanas y puertas que puedan cerrarse con llave deberán haber sido aprobados por la autoridad de seguridad de la Comisión y ofrecer una protección equivalente a la de un contenedor de seguridad aprobado para el almacenamiento de ICUE del mismo grado de clasificación.

*Artículo 19***Medidas de protección física para el manejo y almacenamiento de la ICUE**

1. La ICUE de grado RESTREINT UE/EU RESTRICTED se podrá manejar:
  - a) en una zona de acceso restringido;
  - b) en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas, o
  - c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la ICUE de conformidad con el artículo 31 y se haya comprometido a cumplir las medidas compensatorias establecidas en las normas de desarrollo, para garantizar que la ICUE está protegida del acceso de personas no autorizadas.
2. La ICUE de grado RESTREINT UE/EU RESTRICTED se guardará en muebles de oficina adecuadamente cerrados con llave en las zonas administrativas o las zonas de acceso restringido. La ICUE de dicho grado podrá almacenarse temporalmente fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor se haya comprometido a cumplir las medidas compensatorias establecidas en las normas de desarrollo.
3. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se podrá manejar:
  - a) en una zona de acceso restringido;
  - b) en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas, o
  - c) fuera de una zona de acceso restringido o de una zona administrativa siempre que el poseedor:
    - i) se haya comprometido a cumplir las medidas compensatorias establecidas en las normas de desarrollo para garantizar que el acceso a la ICUE se impide a personas no autorizadas,
    - ii) mantenga la ICUE en todo momento bajo su control personal, y
    - iii) en el caso de documentos en papel, haya notificado el hecho al registro correspondiente.
4. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se almacenará en una zona de acceso restringido dentro de un contenedor de seguridad o una cámara acorazada.
5. La ICUE de nivel TRES SECRET UE/EU TOP SECRET se manejará en una zona de acceso restringido, establecida y mantenida por la autoridad de seguridad de la Comisión, y acreditada a dicho nivel por la Autoridad de Acreditación de Seguridad de la Comisión.
6. La ICUE de nivel TRES SECRET UE/EU TOP SECRET se almacenará en una zona de acceso restringido, a ese nivel, acreditada a dicho nivel por la Autoridad de Acreditación de Seguridad de la Comisión, en una de las condiciones siguientes:
  - a) En un contenedor de seguridad conforme a lo dispuesto en el artículo 18, con al menos uno de los controles adicionales siguientes:
    - 1) protección continua o verificación periódica por personal de seguridad o de servicio habilitado;
    - 2) un SDI aprobado, junto con personal de seguridad para intervención en caso de incidente;o
  - b) en una cámara acorazada con SDI, junto con personal de seguridad para intervención en caso de incidente.

*Artículo 20***Gestión de llaves y combinaciones empleadas para la protección de ICUE**

1. Los procedimientos de gestión de las llaves y combinaciones de las oficinas, salas, cámaras acorazadas y contenedores de seguridad se fijarán en las normas de desarrollo de conformidad con el artículo 60. Estos procedimientos deberán evitar accesos no autorizados.
2. Las combinaciones serán confiadas al menor número posible de personas que necesiten conocerlas. Las combinaciones de los contenedores de seguridad y cámaras acorazadas en los que se guarde ICUE se modificarán:
  - a) al recibir un nuevo contenedor;
  - b) cada vez que cambie el personal que conoce la combinación;
  - c) cada vez que se haya producido o se sospeche que se ha producido una situación de comprometimiento;
  - d) cuando se hayan realizado operaciones de mantenimiento o reparación de una cerradura; y
  - e) al menos cada 12 meses.

## CAPÍTULO 4

## TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA DE LA UE

## Artículo 21

**Principios básicos**

1. Todos los documentos de ICUE deben tratarse con arreglo a la política de la Comisión en materia de gestión de documentos y, en consecuencia, deben registrarse, clasificarse, conservarse y, por último, eliminarse, someterse a muestreo o trasladarse a los archivos históricos de conformidad con la lista común de conservación de expedientes de la Comisión Europea.
2. La información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior se inscribirá en un registro para fines de seguridad antes de ser distribuida y al ser recibida. La información clasificada de grado TRÈS SECRET UE/EU TOP SECRET se inscribirá en registros especiales.
3. En el seno de la Comisión, se establecerá un sistema de registro de la ICUE de conformidad con lo dispuesto en el artículo 27.
4. Los servicios y locales de la Comisión en los que se maneje o almacene ICUE serán inspeccionados periódicamente por la autoridad de seguridad de la Comisión.
5. La transmisión de la ICUE entre los distintos servicios y locales fuera de las zonas físicamente protegidas se llevará a cabo del siguiente modo:
  - a) como norma general, la ICUE se transmitirá por medios electrónicos que estén protegidos con productos criptológicos aprobados de conformidad con lo dispuesto en el capítulo 5;
  - b) en caso de no utilizarse los medios contemplados en la letra a), la ICUE se transportará por cualquiera de los siguientes medios:
    - i) medios electrónicos (por ejemplo, llaves USB, discos compactos o discos duros) que estén protegidos con productos criptológicos aprobados de conformidad con lo dispuesto en el capítulo 5, o
    - ii) en los demás casos, según lo dispuesto en las normas de desarrollo.

## Artículo 22

**Clasificaciones y marcas**

1. La información se clasificará cuando requiera protección respecto de su confidencialidad, de conformidad con lo dispuesto en el artículo 3, apartado 1.
2. El originador de la ICUE será responsable de determinar el grado de clasificación de seguridad atendiendo a las correspondientes normas de desarrollo, normas y directrices en materia de clasificación, y de la difusión inicial de la información.
3. El nivel de clasificación de la ICUE se determinará de conformidad con el artículo 3, apartado 2, y con las normas de desarrollo pertinentes.
4. La clasificación de seguridad se indicará clara y correctamente, independientemente de que la ICUE sea verbal o figure en soporte de papel, electrónico o cualquier otro.
5. Las distintas partes (es decir, páginas, apartados, secciones, anexos, apéndices o documentos adjuntos) de un documento determinado podrán requerir una clasificación diferente, lo cual deberá indicarse en consecuencia, incluso cuando se almacenen en forma electrónica.
6. El grado global de clasificación de un documento o archivo deberá ser al menos tan alto como el de su componente con mayor grado de clasificación. Cuando se recopile información procedente de diversas fuentes, se revisará el producto final para determinar su grado global de clasificación de seguridad, dado que podría estar justificado un grado de clasificación mayor que el de los componentes que lo forman.
7. En la medida de lo posible, los documentos que contengan partes con distintos grados de clasificación se estructurarán de tal modo que las partes con un grado de clasificación diferente puedan ser fácilmente reconocidas y separadas, si fuera necesario.
8. La clasificación de una carta o nota de transmisión de documentos será equivalente al mayor grado de clasificación de los documentos adjuntos. El originador deberá indicar claramente en qué grado está clasificada la información una vez separada de sus documentos adjuntos mediante la marca correspondiente, según el siguiente ejemplo:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sin anexos: RESTREINT UE/EU RESTRICTED

*Artículo 23***Marcas**

Junto con una de las marcas de la clasificación de seguridad fijadas en el artículo 3, apartado 2, la ICUE podrá llevar marcas adicionales tales como:

- a) un identificador para designar al originador;
- b) cualquier advertencia, código o acrónimo que especifique el ámbito de actividad a que se refiere el documento, así como indicaciones relativas a su distribución específica, basada en el principio de la necesidad de conocer, o a restricciones de su uso;
- c) marcas sobre posibilidad de cesión;
- d) en su caso, la fecha o acontecimiento específico tras los cuales podrá rebajarse el grado de clasificación o desclasificarse.

*Artículo 24***Marcas abreviadas de clasificación**

1. Podrán utilizarse marcas abreviadas normalizadas de clasificación para indicar el grado de clasificación de los diferentes apartados de un texto. Las marcas de clasificación completas no se sustituirán por abreviaturas.
2. Podrán utilizarse dentro de documentos clasificados de la UE las siguientes abreviaturas normalizadas para indicar el grado de clasificación de secciones o bloques del texto de extensión inferior a una página:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

*Artículo 25***Producción de ICUE**

1. Cuando se genere un documento clasificado de la UE:
  - a) cada página llevará claramente marcado el grado de clasificación;
  - b) cada página irá numerada;
  - c) el documento deberá llevar un número de referencia y un asunto, que no constituirá en sí mismo información clasificada, salvo que se marque como tal;
  - d) el documento estará fechado;
  - e) los documentos con clasificación SECRET UE/EU SECRET o superior llevarán un número de ejemplar en cada página cuando hayan de distribuirse en varios ejemplares.
2. Cuando no sea posible aplicar el punto 1 a una ICUE, se tomarán otras medidas adecuadas de conformidad con las normas de desarrollo.

*Artículo 26***Reducción del grado de clasificación y desclasificación de la ICUE**

1. En el momento de producir la información, el originador indicará, cuando sea posible, si el grado de clasificación de la ICUE puede ser reducido o desclasificado a partir de una determinada fecha o tras un acontecimiento concreto.
2. Cada servicio de la Comisión revisará periódicamente la ICUE que haya generado para verificar si el grado de clasificación asignado sigue siendo aplicable. Las normas de desarrollo establecerán un sistema para revisar, con una frecuencia mínima quinquenal, el grado de clasificación de la ICUE que se haya generado en la Comisión. Dicha revisión no será necesaria cuando el originador haya indicado desde el principio que el grado de clasificación de la información podrá ser automáticamente reducido o que la información podrá desclasificarse, y la información haya sido marcada consecuentemente.

3. La información clasificada de grado RESTREINT UE/EU RESTRICTED originaria de la Comisión se considerará automáticamente desclasificada después de 30 años, de conformidad con lo dispuesto en el Reglamento (CEE, Euratom) n° 354/83, modificado por el Reglamento (CE, Euratom) n° 1700/2003 del Consejo <sup>(1)</sup>.

#### Artículo 27

##### Sistema de registro de la ICUE en la Comisión

1. Sin perjuicio de lo dispuesto en el artículo 52, apartado 5, en cada servicio de la Comisión donde se maneje o almacene ICUE de nivel CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET, se identificará un responsable local de registro de ICUE para garantizar que la ICUE se maneje de conformidad con las disposiciones de la presente Decisión.
2. El registro de ICUE gestionado por la Secretaría General será el registro central de ICUE de la Comisión, que actuará como:
  - registro local de ICUE para la Secretaría General de la Comisión,
  - registro de ICUE para los gabinetes de los miembros de la Comisión, a menos que estos hayan designado un registro local de ICUE,
  - registro de ICUE para direcciones generales o servicios que no dispongan de un registro local de ICUE,
  - punto principal de entrada y salida de toda la información clasificada de grado RESTREINT UE/EU RESTRICTED y hasta SECRET UE/EU SECRET inclusive, intercambiada entre la Comisión y sus servicios y terceros Estados y organizaciones internacionales, así como, cuando esté previsto en disposiciones específicas, para otras instituciones, órganos u organismos de la Unión.
3. En el seno de la Comisión, la autoridad de seguridad de la Comisión designará un registro para que actúe como principal organismo receptor y emisor de la información clasificada de grado TRÈS SECRET UE/EU TOP SECRET. Cuando proceda, podrán designarse registros secundarios para manejar dicha información.
4. Los registros secundarios no podrán transmitir documentos TRÈS SECRET UE/EU TOP SECRET directamente a otros registros secundarios dependientes del mismo registro central TRÈS SECRET UE/EU TOP SECRET ni al exterior sin la aprobación expresa por escrito de este último.
5. Los registros de ICUE se constituirán como zonas de acceso restringido, según lo definido en el capítulo 3, y acreditados por la Autoridad de Acreditación de Seguridad (AAS).

#### Artículo 28

##### Controlador del registro

1. Cada registro de ICUE será gestionado por un controlador del registro («RCO»).
2. Los RCO deberán tener la debida habilitación de seguridad.
3. Los RCO estarán sujetos a la supervisión del LSO en los servicios de la Comisión por lo que respecta a la aplicación de las disposiciones sobre el tratamiento de los documentos de ICUE y el cumplimiento de las normas, estándares y directrices de seguridad pertinentes.
4. En el ámbito de su responsabilidad de gestionar el registro de ICUE al que haya sido asignado, el RCO deberá asumir las siguientes tareas de conformidad con lo dispuesto en la presente Decisión y en las correspondientes normas de desarrollo, estándares y directrices:
  - gestionar las operaciones relativas al registro, conservación, reproducción, traducción, envío y destrucción, o traslado al servicio de archivos históricos de la ICUE,
  - comprobar periódicamente la necesidad de mantener la clasificación de la información,
  - asumir las demás tareas relacionadas con la protección de la ICUE definidas en las normas de desarrollo.

#### Artículo 29

##### Registro de la ICUE a efectos de seguridad

1. A efectos de la presente Decisión, por registro a efectos de seguridad (en lo sucesivo denominado «registro») se entenderá la aplicación de procedimientos que registren el ciclo de vida de la ICUE, incluida su difusión.

<sup>(1)</sup> Reglamento (CE, Euratom) n° 1700/2003 del Consejo, de 22 de septiembre de 2003, por el que se modifica el Reglamento (CEE, Euratom) n° 354/83 relativo a la apertura al público de los archivos históricos de la Comunidad Económica Europea y de la Comunidad Europea de la Energía Atómica (DO L 243 de 27.9.2003, p. 1).

2. Toda la información o el material clasificado de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior se inscribirá en registros especiales a su recepción o envío de una entidad organizativa.
3. Cuando se maneje o almacene ICUE utilizando un sistema de información y comunicación (SIC), los procedimientos de registro podrán llevarse a cabo mediante procesos dentro del propio SIC.
4. En las normas de desarrollo se establecerán disposiciones más detalladas sobre el registro de ICUE a efectos de seguridad.

#### Artículo 30

##### **Copia y traducción de documentos clasificados de la UE**

1. Los documentos TRÈS SECRET UE/EU TOP SECRET solo podrán copiarse o traducirse con el consentimiento previo por escrito del originador.
2. Cuando el originador de documentos clasificados de grado SECRET UE/EU SECRET o inferior no haya impuesto ninguna restricción a su copia o traducción, estos documentos podrán copiarse o traducirse por orden de su poseedor.
3. Las medidas de seguridad aplicables a los documentos originales serán aplicables a sus copias y traducciones.

#### Artículo 31

##### **Transporte de ICUE**

1. La ICUE se transportará de forma que esté protegida frente a la divulgación no autorizada durante su transporte.
2. El transporte de ICUE estará sujeto a medidas de protección que deberán:
  - ser acordes con el nivel de clasificación de la ICUE transportada,
  - estar adaptadas a las condiciones específicas de su transporte, especialmente en función de si la ICUE se transporta:
    - dentro de un edificio o de un grupo independiente de edificios de la Comisión,
    - entre edificios de la Comisión situados en el mismo Estado miembro;
    - dentro de la Unión,
    - desde la Unión al territorio de un tercer Estado, y
    - estar adaptadas a la naturaleza y forma de la ICUE.
3. Dichas medidas de protección se establecerán en detalle en las normas de desarrollo o, en el caso de los proyectos y programas a que se refiere el artículo 42, como parte integrante de las instrucciones de seguridad de un programa o proyecto.
4. Las normas de desarrollo o las instrucciones de seguridad de un programa o proyecto deberán incluir disposiciones en relación con el nivel de la ICUE, por lo que se refiere a:
  - el tipo de transporte, tal como transporte en mano, correo diplomático o militar, transporte por servicios postales o servicios de mensajería comercial,
  - el empaquetado de la ICUE,
  - contramedidas técnicas para la ICUE que se transporte por medios electrónicos,
  - cualquier otra medida de procedimiento, física o electrónica,
  - procedimientos de registro,
  - el recurso a personal de seguridad autorizado.
5. Cuando se transmita ICUE por medios electrónicos, y no obstante lo dispuesto en el artículo 21, apartado 5, las medidas de protección establecidas en las normas de desarrollo pertinentes se completarán con las debidas contramedidas técnicas aprobadas por la autoridad de seguridad de la Comisión a fin de reducir al mínimo el riesgo de pérdida o comprometimiento.

*Artículo 32***Destrucción de ICUE**

1. Los documentos clasificados de la UE que hayan dejado de ser necesarios podrán destruirse, teniendo en cuenta las normas sobre archivos y las normas y reglamentos de la Comisión en materia de gestión de documentos y archivo, y en particular la lista común de conservación de la Comisión.
2. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL y superior será destruida por el RCO del registro responsable de la ICUE por orden de su poseedor o de una autoridad competente. El RCO deberá actualizar en consecuencia los libros de registro y cualquier información relacionada con el registro.
3. Cuando se trate de documentos clasificados de grado SECRET UE/EU SECRET o TRÈS SECRET UE/EU TOP SECRET, la destrucción la realizará el RCO en presencia de un testigo, que deberá estar habilitado como mínimo para el grado de clasificación del documento que se vaya a destruir.
4. El encargado del registro, y el testigo en caso de que se requiera su presencia, firmarán un certificado de destrucción, que se archivará en el registro. El RCO del registro responsable de la ICUE conservará los certificados de destrucción de los documentos de grado TRES SECRET UE/EU TOP SECRET durante un período de 10 años como mínimo, y de los documentos con clasificación CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante 5 años como mínimo.
5. Los documentos clasificados, incluidos los de nivel RESTREINT UE/EU RESTRICTED, se destruirán por métodos que se definirán en las normas de desarrollo y que cumplirán las normas de la Unión pertinentes o normas equivalentes.
6. Los soportes de almacenamiento informático utilizados para la ICUE se destruirán con arreglo a procedimientos establecidos en las normas de desarrollo.

*Artículo 33***Destrucción de ICUE en situaciones de urgencia**

1. Los servicios de la Comisión que tengan EUCI prepararán planes basados en las condiciones locales para proteger el material clasificado de la UE en situaciones de crisis, incluidos, si fuera necesario, planes de destrucción y evacuación de urgencia. Promulgarán las instrucciones que se estimen necesarias para impedir que la ICUE caiga en manos de personas no autorizadas.
2. Las disposiciones para la salvaguardia o la destrucción de material CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET en una crisis no afectarán en ningún caso a la salvaguardia o destrucción de material TRÈS SECRET UE/EU TOP SECRET, incluido el equipo de mensajes cifrados, cuyo tratamiento debe tener prioridad sobre todas las demás tareas.
3. En caso de urgencia, y de haber un riesgo inminente de revelación no autorizada, la ICUE será destruida por el poseedor, de tal modo que no pueda reconstruirse ni total ni parcialmente. Se informará al originador y al registro originador de la destrucción de urgencia de la ICUE registrada.
4. En las normas de desarrollo se establecerán disposiciones más detalladas para la destrucción de ICUE.

## CAPÍTULO 5

**PROTECCIÓN DE INFORMACIÓN CLASIFICADA DE LA UE EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (SIC)***Artículo 34***Principios básicos de garantía de la información**

1. Por «garantía de la información» (GI) en el ámbito de los sistemas de información y comunicaciones, se entenderá la confianza en que esos sistemas protejan la información que manejan y funcionen como es necesario que lo hagan, cuando así se precise, bajo el control de sus legítimos usuarios.

2. Una GI efectiva habrá de garantizar unos niveles apropiados de:

Autenticidad: la garantía de que la información es verídica y procede de fuentes de buena fe.

Disponibilidad: la propiedad de ser accesible y utilizable en el momento que lo requiera una entidad autorizada.

Confidencialidad: la propiedad de la información de no ser revelada a personas, organismos o procesos no autorizados.

Integridad: la propiedad de salvaguardar la exactitud y completitud de la información y los activos.

No repudio: la capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente.

3. La GI se basará en un proceso de gestión de riesgos.

#### Artículo 35

### Definiciones

A efectos del presente capítulo, se entenderá por:

- a) «Acreditación»: autorización formal y aprobación concedidas a un sistema de información y comunicaciones por la Autoridad de Acreditación de Seguridad (AAS) para tratar ICUE en su entorno operativo, tras la validación formal del plan de seguridad y su correcta aplicación.
- b) «Proceso de acreditación»: medidas necesarias y tareas requeridas con anterioridad a la acreditación por la AAS. Estas medidas y tareas se especificarán en una norma del proceso de acreditación.
- c) «Sistema de información y comunicaciones» (SIC): sistema que permite manejar información en formato electrónico. Abarca todos los medios necesarios para su funcionamiento, incluidos la infraestructura, la organización y los recursos de personal e información.
- d) «Riesgo residual»: riesgo que persiste una vez aplicadas las medidas de seguridad, dado que no es posible contrarrestar todas las amenazas ni eliminar todas las vulnerabilidades.
- e) «Riesgo»: posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades internas o externas de una organización o de cualquier sistema que esta utilice y al hacerlo ocasione daños a la organización o a sus activos tangibles o intangibles. Se mide como la combinación de la probabilidad de que se cumplan las amenazas y de su repercusión.
- f) «Aceptación del riesgo»: decisión de aceptar, una vez tratado el riesgo, la persistencia de un riesgo residual.
- g) «Evaluación del riesgo»: determinación de las amenazas y vulnerabilidades y realización del correspondiente análisis del riesgo, es decir, el análisis de la probabilidad y las repercusiones.
- h) «Comunicación del riesgo»: sensibilización sobre los riesgos a las comunidades de usuarios de SIC e información sobre tales riesgos a las autoridades responsables de la aprobación y a las autoridades operativas.
- i) «Tratamiento del riesgo»: atenuación, supresión o reducción del riesgo (adoptando una combinación adecuada de medidas técnicas, físicas, de gestión o de procedimiento), transferencia del riesgo o seguimiento del mismo.

#### Artículo 36

### SIC que manejen ICUE

1. Los SIC manejarán la ICUE de conformidad con el concepto de GI.

2. Para los SIC que manejen ICUE, el cumplimiento de la política de seguridad de los sistemas de información de la Comisión, tal como se establece en la Decisión de la Comisión C(2006) 3602, implica que <sup>(1)</sup>:

- a) se aplicará el enfoque «planear-ejecutar-verificar-actuar» a la ejecución de la política de seguridad de los sistemas de información durante todo el ciclo de vida del sistema de información;
- b) las necesidades en materia de seguridad deberán determinarse a partir de una evaluación del impacto en la actividad;
- c) el sistema de información y los datos que contiene deberán someterse a una clasificación formal de los activos;

<sup>(1)</sup> C(2006) 3602, de 16 de agosto de 2006, relativa a la seguridad de los sistemas de información utilizados por la Comisión Europea.



- d) las medidas de protección obligatorias determinadas por la política de seguridad de los sistemas de información deberán ponerse en práctica;
- e) deberá aplicarse un proceso de gestión de riesgos, que consta de las siguientes etapas: identificación de amenazas y vulnerabilidades, evaluación del riesgo, gestión del riesgo, aceptación del riesgo y comunicación del riesgo;
- f) se definirá, aplicará, verificará y revisará un plan de seguridad que incluya la política de seguridad y los procedimientos operativos de seguridad.
3. Todo el personal involucrado en el diseño, desarrollo, prueba, operación, gestión o utilización de los SIC que manejen ICUE notificará a la AAS todos los posibles puntos débiles, incidentes, fallos de seguridad o comprometimientos que puedan tener un impacto en la protección del SIC o de la ICUE que contenga.
4. Cuando la protección de la ICUE se realice mediante productos criptológicos, dichos productos se aprobarán del siguiente modo:
- a) se dará preferencia a los productos que hayan sido aprobados por el Consejo o por el Secretario General del Consejo, en su calidad de autoridad de certificación criptológica del Consejo, por recomendación del grupo de expertos de seguridad de la Comisión;
- b) cuando ello esté justificado por motivos operativos específicos, la Autoridad de Certificación Criptológica de la Comisión (ACC) podrá, por recomendación del grupo de expertos de seguridad de la Comisión, dispensar del cumplimiento de los requisitos a que se refiere la letra a) y otorgar una aprobación provisional durante un período específico.
5. Durante la transmisión, tratamiento y almacenamiento de la ICUE por medios electrónicos se emplearán productos criptográficos homologados. Sin perjuicio de este requisito, se podrán aplicar procedimientos específicos en circunstancias urgentes o en configuraciones técnicas específicas previa aprobación de la ACC.
6. Se aplicarán medidas de seguridad a fin de proteger los SIC que manejen información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o superior de modo que dicha información no pueda verse comprometida como consecuencia de emanaciones electromagnéticas no intencionadas («medidas de seguridad TEMPEST»). Estas medidas de seguridad serán proporcionadas al riesgo de explotación de la información y al grado de clasificación de esta.
7. La autoridad de seguridad de la Comisión asumirá las funciones siguientes:
- Autoridad de Garantía de la Información (AGI),
  - Autoridad de Acreditación de Seguridad (AAS),
  - Autoridad TEMPEST,
  - Autoridad de Certificación Criptológica (ACC),
  - Autoridad de Distribución Criptológica (ADC).
8. La autoridad de seguridad de la Comisión designará para cada sistema a la Autoridad Operacional de Garantía de la Información (AOGI).
9. Las responsabilidades de las funciones descritas en los apartados 7 y 8 se determinarán en las normas de desarrollo.

#### Artículo 37

#### **Acreditación de los SIC que manejen ICUE**

1. Todos los SIC que manejen ICUE serán objeto de un proceso de acreditación, basado en los principios de la GI, cuyo nivel de detalle debe ser acorde con el nivel de protección requerido.
2. El proceso de acreditación incluirá la validación formal por la AAS de la Comisión del plan de seguridad para el SIC de que se trate a fin de obtener garantías de que:
- a) se ha llevado a cabo de forma apropiada el proceso de gestión de riesgos, según lo indicado en el artículo 36, apartado 2;
- b) el propietario del sistema ha asumido conscientemente el riesgo residual, y
- c) se ha alcanzado un nivel de protección suficiente del SIC y de la ICUE manejada en él, de conformidad con la presente Decisión.

3. La AAS de la Comisión expedirá una declaración de acreditación que determinará el nivel máximo de clasificación de la ICUE que pueda manejarse en el SIC, así como las condiciones correspondientes para la operación. Esto se entenderá sin perjuicio de las tareas encomendadas al Consejo de Acreditación de Seguridad definido en el artículo 11 del Reglamento (UE) nº 512/2014 del Parlamento Europeo y del Consejo (<sup>1</sup>).
4. Un Consejo de Acreditación de Seguridad conjunto se encargará de la acreditación de los SIC de la Comisión en los que participen varias partes. Estará integrado por un representante de la AAS de cada parte, y lo presidirá un representante de la AAS de la Comisión.
5. El proceso de acreditación constará de una serie de tareas que deberán asumir las partes interesadas. La responsabilidad de la preparación de los expedientes de acreditación y la documentación será plenamente del propietario del SIC.
6. La acreditación será competencia de la AAS de la Comisión, que, en cualquier momento en el ciclo de vida del SIC, tendrá derecho a:
  - a) exigir que se aplique un proceso de acreditación;
  - b) auditar o inspeccionar el SIC;
  - c) cuando dejen de cumplirse las condiciones de funcionamiento, exigir la definición y aplicación efectiva de un plan de mejora de la seguridad en un plazo bien definido, pudiendo retirar el permiso para operar el SIC hasta que se cumplan de nuevo las condiciones para la operación.
7. El proceso de acreditación se establecerá en una norma sobre el proceso de acreditación de los SIC que manejen ICUE, que deberá adoptarse de conformidad con el artículo 10, apartado 3, de la Decisión C(2006) 3602.

#### Artículo 38

### Circunstancias de urgencia

1. No obstante lo dispuesto en el presente capítulo, podrán aplicarse los procedimientos específicos que se describen a continuación en casos de urgencia, por ejemplo, en situaciones de crisis, conflicto o guerra, inminentes o reales, o en circunstancias operativas excepcionales.
2. La ICUE podrá transmitirse utilizando productos criptológicos que hayan sido certificados para un grado de clasificación inferior o sin cifrar con el consentimiento de la autoridad competente, si resulta evidente que un retraso podría causar un daño superior al que acarrea la revelación del material clasificado y si:
  - a) el emisor y el receptor carecen de los medios de cifra requeridos, y
  - b) el material clasificado no puede transmitirse a tiempo por otros medios.
3. En las circunstancias expuestas en el apartado 1, la información clasificada transmitida no llevará ninguna marca ni indicación que la distinga de la información no clasificada o que pueda protegerse mediante un producto criptológico disponible. Se notificará sin demora a los receptores el grado de clasificación, recurriendo a otros medios.
4. Se presentará posteriormente un informe a la autoridad competente y al grupo de expertos de seguridad de la Comisión.

#### CAPÍTULO 6

### SEGURIDAD INDUSTRIAL

#### Artículo 39

### Principios básicos

1. Por «seguridad industrial» se entenderá la aplicación de medidas encaminadas a garantizar la protección de la ICUE:
  - a) en el marco de los contratos clasificados, por:
    - i) los candidatos o licitadores a lo largo de todo el procedimiento de licitación y contratación,
    - ii) los contratistas o subcontratistas durante toda la vigencia de los contratos clasificados;

(<sup>1</sup>) Reglamento (UE) nº 512/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por el que se modifica el Reglamento (UE) nº 912/2010, por el que se crea la Agencia del GNSS Europeo (DO L 150 de 20.5.2014, p. 72).

- b) en el marco de los acuerdos de subvención clasificados, por:
  - i) los solicitantes durante los procedimientos de concesión de subvenciones;
  - ii) los beneficiarios a lo largo de todo el ciclo de vida de los acuerdos de subvención clasificados.
2. Dichos contratos o acuerdos de subvención no implicarán información clasificada TRES SECRET UE/EU TOP SECRET.
3. Salvo indicación en contrario, las disposiciones del presente capítulo relativas a contratos clasificados o contratistas serán también aplicables a los subcontratos clasificados o subcontratistas.

#### Artículo 40

### Definiciones

A efectos del presente capítulo se entenderá por:

- a) «Contrato clasificado»: contrato marco o contrato, conforme a lo dispuesto en el Reglamento (CE, Euratom) nº 1605/2002 de la Comisión <sup>(1)</sup>, firmado por la Comisión o uno de sus servicios con un contratista para el suministro de bienes muebles o inmuebles, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.
- b) «Subcontrato clasificado»: contrato celebrado por un contratista de la Comisión o alguno de sus servicios, con otro contratista (denominado «subcontratista») para el suministro de bienes muebles o inmuebles, la ejecución de obras o la prestación de servicios cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.
- c) «Acuerdo de subvención clasificado»: acuerdo en virtud del cual la Comisión concede una subvención, tal como se indica en la parte I, título VI, del Reglamento (CE, Euratom) nº 1605/2002, cuya ejecución exija o implique la creación, manipulación o almacenamiento de ICUE.
- d) «Autoridad de Seguridad Designada» (ASD): autoridad responsable ante la Autoridad Nacional de Seguridad (ANS) de un Estado miembro, encargada de comunicar a las sociedades industriales u otro tipo de entidades la política nacional en todos los aspectos de la seguridad industrial y de facilitarles dirección y asistencia para su aplicación. La función de ASD podrá ser ejercida por la ANS o por cualquier otra autoridad competente.

#### Artículo 41

### Procedimiento para los contratos o acuerdos de subvención clasificados

1. Cada servicio de la Comisión, en calidad de órgano de contratación, velará por que las normas mínimas sobre seguridad industrial establecidas en el presente capítulo se mencionen o incorporen en el contrato, y se cumplan, a la hora de adjudicar contratos o acuerdos de subvención clasificados.
2. A efectos de lo dispuesto en el apartado 1, los servicios competentes de la Comisión solicitarán el dictamen de la Dirección General de Recursos Humanos y Seguridad, y, en particular, de su Dirección de Seguridad, y velarán por que los modelos de contratos y subcontratos y los modelos de acuerdos de subvención incluyan disposiciones que reflejen los principios básicos y las normas mínimas de protección de la ICUE que deben cumplir los contratistas y subcontratistas, y los beneficiarios de acuerdos de subvención, respectivamente.
3. La Comisión cooperará estrechamente con la ANS, la ASD o cualquier otra autoridad competente de los Estados miembros de que se trate.
4. Cuando un órgano de contratación se proponga poner en marcha un procedimiento destinado a celebrar un contrato o un acuerdo de subvención clasificado, solicitará el dictamen de la autoridad de seguridad de la Comisión sobre cuestiones relativas a la naturaleza y elementos clasificados del procedimiento, en todas sus fases.
5. En las normas de desarrollo sobre seguridad industrial, previa consulta al grupo de expertos de seguridad de la Comisión, se establecerán plantillas y modelos de contratos y subcontratos clasificados, acuerdos de subvención clasificados, anuncios de contrato, orientación sobre las circunstancias en que se requiere una habilitación de seguridad de establecimiento, instrucciones de seguridad de un programa o proyecto, cláusulas sobre aspectos de la seguridad, visitas, y transmisión y transporte de ICUE en virtud de contratos o acuerdos de subvención clasificados.

<sup>(1)</sup> Reglamento (CE, Euratom) nº 1605/2002 del Consejo, de 25 de junio de 2002, por el que se aprueba el Reglamento financiero aplicable al presupuesto general de las Comunidades Europeas (DO L 248 de 16.9.2002, p. 1).

6. La Comisión podrá celebrar contratos o acuerdos de subvención clasificados que conlleven tareas que conlleven el acceso a ICUE o su manejo o almacenamiento por operadores económicos registrados en un Estado miembro o en un tercer Estado con los que se haya celebrado un acuerdo o un convenio administrativo de conformidad con lo dispuesto en el capítulo 7 de la presente Decisión.

#### Artículo 42

### Elementos de seguridad en un contrato o acuerdo de subvención clasificado

1. Los contratos o contratos de subvención clasificados incluirán los siguientes elementos de seguridad:

#### Instrucciones de seguridad de un programa o proyecto

- a) Las «Instrucciones de seguridad de un programa o proyecto» son una lista de procedimientos de seguridad aplicables a un programa o proyecto específico para tipificar los procedimientos de seguridad. Pueden ser objeto de revisión a lo largo de la ejecución del programa o proyecto.
- b) La Dirección General de Recursos Humanos y Seguridad elaborará Instrucciones de seguridad de un programa o proyecto genéricas. Los servicios de la Comisión responsables de los programas o proyectos que conlleven el manejo o almacenamiento de ICUE podrán desarrollar, cuando proceda, instrucciones específicas, que se basarán en dichas instrucciones genéricas.
- c) Se desarrollarán Instrucciones de seguridad de un programa o proyecto, en particular, para programas y proyectos caracterizados por su gran alcance, importancia o complejidad, o por la multiplicidad o diversidad de los contratistas, beneficiarios y otros socios y partes interesadas, por ejemplo en lo que respecta a su situación jurídica. La Instrucciones de seguridad de un programa o proyecto serán elaboradas por el servicio o servicios de la Comisión que gestionen el programa o proyecto, en estrecha colaboración con la Dirección General de Recursos Humanos y Seguridad.
- d) La Dirección General de Recursos Humanos y Seguridad someterá a la apreciación del grupo de expertos de seguridad de la Comisión tanto las Instrucciones de seguridad de un programa o proyecto genéricas como las específicas.

#### Cláusula sobre aspectos de la seguridad

- a) «Cláusula sobre aspectos de la seguridad»: conjunto de condiciones contractuales especiales impuestas por el órgano de contratación y que forman parte integrante de un contrato clasificado que conlleve el acceso a ICUE o la creación de ese tipo de información; en ella se enumeran los requisitos de seguridad o los elementos del contrato que requieren protección de seguridad.
- b) Los requisitos de seguridad específicos de un contrato se describirán en una cláusula sobre aspectos de seguridad, la cual, cuando proceda, incluirá la guía de clasificación de la seguridad y será parte integrante de un contrato o subcontrato o acuerdo de subvención clasificado.
- c) La cláusula sobre aspectos de la seguridad incluirá asimismo las disposiciones que exigirán del contratista o subcontratista el cumplimiento de los estándares mínimos que se establecen en la presente Decisión. El órgano de contratación se asegurará de que la cláusula indique que el incumplimiento de dichos estándares mínimos podrá ser motivo suficiente para la rescisión del contrato o del acuerdo de subvención.

2. Tanto las Instrucciones de seguridad de un programa o proyecto como las cláusulas sobre aspectos de la seguridad incluirán como elemento de seguridad obligatorio una guía de clasificación de seguridad:

- a) «Guía de clasificación de seguridad»: documento que describe los elementos de un programa, proyecto, contrato o acuerdo de subvención que están clasificados, con especificación de los grados de clasificación de seguridad aplicables. La guía podrá ampliarse durante toda la vigencia del programa, proyecto, contrato o acuerdo de subvención, y se podrá reducir el grado de clasificación o reclasificar los elementos de información; cuando exista una guía, formará parte de la cláusula sobre aspectos de la seguridad.
- b) Antes de convocar una licitación o adjudicar un contrato clasificado, el servicio de la Comisión, como órgano de contratación, determinará la clasificación de seguridad de toda información que deba proporcionarse a los candidatos y licitadores o contratistas, así como la clasificación de seguridad de toda información que haya de producir el contratista. Para ello, elaborará una guía de clasificación de la seguridad, que deberá emplearse en la ejecución del contrato, con arreglo a lo dispuesto en la presente Decisión y sus normas de desarrollo, previa consulta a la autoridad de seguridad de la Comisión.

- c) Para determinar la clasificación de seguridad de los diversos elementos de un contrato clasificado se aplicarán los principios siguientes:
- i) al elaborar una guía de clasificación de seguridad, el servicio de la Comisión, como órgano de contratación, tendrá en cuenta todos los aspectos de seguridad pertinentes, incluida la clasificación de seguridad atribuida a la información que se facilite y apruebe para ser utilizada en el contrato en cuestión por el originador de la información;
  - ii) el grado general de clasificación del contrato no podrá ser inferior al mayor grado de clasificación de cualquiera de sus elementos; y
  - iii) cuando proceda, en caso de que se produzca algún cambio en relación con la clasificación de la información producida por los contratistas o que se les haya facilitado en la ejecución de un contrato, y cuando se introduzca cualquier cambio ulterior en la guía de clasificación de seguridad, el órgano de contratación, a través de la autoridad de seguridad de la Comisión, actuará de enlace con las ANS o las ASD de los Estados miembros o cualquier otra autoridad nacional de seguridad afectada.

#### Artículo 43

### Acceso a la ICUE del personal de los beneficiarios y los contratistas

El órgano de contratación o la autoridad que concede la subvención se asegurará de que el contrato o acuerdo de subvención clasificado incluya disposiciones que indiquen que al personal del contratista, subcontratista o beneficiario que, para la ejecución del contrato, subcontrato o acuerdo de subvención clasificado, precise el acceso a ICUE, solo se le concederá dicho acceso si:

- a) la persona posee una autorización de seguridad para el nivel adecuado u otra autorización debidamente emitida para la que se haya comprobado su necesidad de conocer la información;
- b) ha sido instruida sobre las normas de seguridad aplicables para la protección de la ICUE, y ha aceptado sus responsabilidades en lo que respecta a la protección de dicha información;
- c) ha sido habilitada para el nivel correspondiente para la información clasificada de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET por la ANS, la ASD o cualquier otra autoridad competente.

#### Artículo 44

### Habilitación de seguridad de establecimiento

1. «Habilitación de seguridad de establecimiento»: certificación administrativa por parte de una ANS o ASD o cualquier otra autoridad de seguridad competente de que, desde el punto de vista de la seguridad, un determinado establecimiento puede brindar un nivel adecuado de protección a la ICUE de un grado específico de clasificación de seguridad.

2. La habilitación de seguridad de establecimiento concedida por la ANS, la ASD o cualquier otra autoridad de seguridad competente de un Estado miembro para indicar, de conformidad con las disposiciones legales y reglamentarias nacionales, que un operador económico puede proteger la ICUE del nivel de clasificación que corresponda (CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET) en sus instalaciones, deberá presentarse a la autoridad de seguridad de la Comisión, que la remitirá al servicio de la Comisión que actúe como órgano de contratación o autoridad que concede la subvención, antes de que pueda facilitarse acceso a la ICUE a un candidato, licitador o contratista, o solicitante o beneficiario de la subvención.

3. En su caso, el órgano de contratación notificará, a través de la autoridad de seguridad de la Comisión, la ANS adecuada, la ASD o cualquier otra autoridad de seguridad competente, que es necesario contar con una habilitación de seguridad de establecimiento para la ejecución del contrato. Se exigirá una habilitación de seguridad de establecimiento o una HPS en los casos en que, en el transcurso del procedimiento de adjudicación de contratos o de concesión de subvenciones, deba facilitarse ICUE clasificada en el nivel CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET.

4. El órgano de contratación o la autoridad que conceda la subvención no adjudicará un contrato o un acuerdo de subvención clasificado al licitador seleccionado antes de haber recibido de la ANS, de la ASD o de cualquier otra autoridad de seguridad competente del Estado miembro en que esté registrado el contratista o subcontratista confirmación de que se ha expedido a este la habilitación de seguridad de establecimiento adecuada.

5. La ANS, la ASD o cualquier otra autoridad de seguridad competente que haya expedido una habilitación de seguridad de establecimiento notificará a la autoridad de seguridad de la Comisión los cambios que afecten a dicha habilitación. Esta autoridad, a su vez, informará de ello al servicio de la Comisión que actúe como órgano de contratación o autoridad que concede la subvención. En el caso de los subcontratos, se informará al respecto a la ANS, la ASD o cualquier otra autoridad de seguridad competente.

6. La retirada de una habilitación de seguridad de establecimiento por parte de la ANS, la ASD o cualquier otra autoridad de seguridad competente constituirá motivo suficiente para que el órgano de contratación o la autoridad que concede la subvención rescinda un contrato clasificado o excluya a un licitador de la licitación. Se incluirá una disposición a tal efecto en el modelo de contratos y acuerdos de subvención que se desarrollen.

#### Artículo 45

##### Disposiciones para contratos y acuerdos de subvención clasificados

1. Cuando se facilite ICUE a un candidato, licitador o solicitante durante el procedimiento de licitación, la convocatoria de licitación o convocatoria de propuestas deberá contener una cláusula que obligue a los candidatos, licitadores o solicitantes que no presenten una oferta o propuesta o que no resulten seleccionados a devolver toda la documentación clasificada en un plazo determinado.
2. El órgano de contratación o la autoridad que concede la subvención notificará, a través de la autoridad de seguridad de la Comisión, a la ANS competente, la ASD o cualquier otra autoridad de seguridad competente, el hecho de que se ha adjudicado un contrato o un acuerdo de subvención, y los datos pertinentes, tales como el nombre del contratista o contratistas o los beneficiarios, la duración del contrato y el nivel máximo de clasificación.
3. Cuando tales contratos o acuerdos de subvención finalicen, el órgano de contratación o la autoridad que concede la subvención lo notificará sin demora, a través de la autoridad de seguridad de la Comisión, a la ANS, la ASD o cualquier otra autoridad de seguridad competente del Estado miembro en que esté registrado el contratista o el beneficiario de la subvención.
4. Por regla general, el contratista o el beneficiario de la subvención estará obligado a devolver al órgano de contratación o la autoridad que concede la subvención, al término del contrato clasificado o del acuerdo de subvención, o de la participación de un beneficiario de la subvención, toda la ICUE que obre en su posesión.
5. En la cláusula sobre aspectos de la seguridad se incluirán disposiciones específicas para la eliminación de ICUE durante la ejecución del contrato clasificado o el acuerdo de subvención clasificado.
6. En caso de que el contratista o el beneficiario de la subvención esté autorizado para conservar ICUE al término de un contrato o acuerdo de subvención clasificado, las normas mínimas contenidas en la presente Decisión seguirán siendo de obligado cumplimiento y la confidencialidad de la ICUE será protegida por el titular del contrato o el beneficiario de la subvención.

#### Artículo 46

##### Disposiciones específicas para los contratos clasificados

1. Las condiciones pertinentes para la protección de la ICUE en que un contratista podrá subcontratar se definirán en el pliego de condiciones y en el contrato.
2. Antes de subcontratar cualquier parte de un contrato clasificado, el contratista deberá obtener el permiso correspondiente del órgano de contratación. No podrá adjudicarse un subcontrato que implique el acceso a ICUE a subcontratistas registrados en un tercer país, salvo si existe un marco reglamentario para la seguridad de la información con arreglo a lo dispuesto en el capítulo 7.
3. El contratista responderá de que todas las actividades subcontratadas se ejecuten de conformidad con las normas mínimas prescritas en la presente Decisión y no transmitirá ICUE a ningún subcontratista sin el previo consentimiento escrito del órgano de contratación.
4. Respecto de la ICUE producida o manejada por el contratista, la Comisión será considerada el originador, y los derechos que asistan al originador serán ejercidos por el órgano de contratación.

#### Artículo 47

##### Visitas en relación con contratos clasificados

1. Cuando el personal de la Comisión, de los contratistas o de los beneficiarios de subvenciones necesite acceder a información clasificada de los grados CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET que se halle en los locales de los otros para la ejecución de un contrato o un acuerdo de subvención clasificado, se organizarán visitas, en contacto con las ANS, las ASD o cualquier otra autoridad de seguridad competente. La autoridad de seguridad de la Comisión será informada de dichas visitas. Sin embargo, en el contexto de programas o proyectos específicos, las ANS, las ASD o cualquier otra autoridad de seguridad competente también podrán acordar un procedimiento que permita organizar directamente dichas visitas.

2. Todos los visitantes deberán estar en posesión de una habilitación de seguridad adecuada y tener necesidad de conocer para poder acceder a la ICUE relacionada con el contrato clasificado.
3. A los visitantes solo se les permitirá el acceso a ICUE que guarde relación con la finalidad de la visita.
4. En las normas de desarrollo se establecerán disposiciones más detalladas.
5. Será obligatorio el cumplimiento de las disposiciones en materia de visitas en relación con los contratos clasificados establecidas en la presente Decisión y en las normas de desarrollo a que se refiere el apartado 4.

#### Artículo 48

##### **Transmisión y transporte de ICUE en relación con contratos clasificados o acuerdos de subvención clasificados**

1. Por lo que se refiere a la transmisión de ICUE por medios electrónicos, se aplicarán las disposiciones pertinentes del capítulo 5 de la presente Decisión.
2. Por lo que se refiere al transporte de ICUE, se aplicarán las disposiciones pertinentes del capítulo 4 de la presente Decisión y sus normas de desarrollo, de conformidad con las disposiciones legales y reglamentarias nacionales.
3. Por lo que se refiere al transporte como carga de material clasificado, se aplicarán los siguientes principios para determinar las medidas de seguridad:
  - a) la seguridad deberá estar garantizada durante todas las fases del transporte, desde el punto de origen hasta el destino final;
  - b) el grado de protección concedido a un envío se determinará en función del mayor grado de clasificación del material que contenga;
  - c) antes de efectuarse cualquier traslado transfronterizo de material clasificado de los grados CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, el remitente elaborará un plan de transporte que deberá ser aprobado por la ANS, la ASD o cualquier otra autoridad de seguridad competente afectada;
  - d) en la medida de lo posible, los viajes evitarán las paradas intermedias y se completarán con toda la rapidez que las circunstancias permitan;
  - e) siempre que sea posible, se circulará exclusivamente a través de Estados miembros. Solo deberán emplearse itinerarios que atraviesen Estados no miembros de la UE previa autorización de la ANS, la ASD o cualquier otra autoridad de seguridad competente tanto del Estado remitente como del destinatario.

#### Artículo 49

##### **Transmisión de ICUE a contratistas o beneficiarios de subvenciones establecidos en terceros Estados**

La ICUE se transmitirá a los beneficiarios de subvenciones o contratistas establecidos en terceros Estados de conformidad con las medidas de seguridad acordadas entre la autoridad de seguridad de la Comisión, el servicio de la Comisión como órgano de contratación o autoridad que concede la subvención, y la ANS, la ASD o cualquier otra autoridad de seguridad competente del Estado tercero en el que esté registrado el contratista o el beneficiario de la subvención.

#### Artículo 50

##### **Manejo de información clasificada con grado RESTREINT UE/EU RESTRICTED en el contexto de los contratos clasificados o los acuerdos de subvención clasificados**

1. La protección de información clasificada de grado RESTREINT UE/EU RESTRICTED manejada o almacenada en virtud de contratos o acuerdos de subvención clasificados se basará en los principios de proporcionalidad y de relación coste-eficacia.
2. No se exigirá la habilitación de seguridad de establecimiento ni una HPS en el contexto de los contratos clasificados o los acuerdos de subvención clasificados que impliquen el manejo de información clasificada en el nivel RESTREINT UE/EU RESTRICTED.
3. Cuando un contrato o acuerdo de subvención implique el manejo de información clasificada de grado RESTREINT UE/EU RESTRICTED en un SIC gestionado por un contratista o beneficiario de una subvención, el órgano de contratación o la autoridad que concede la subvención deberá garantizar, previa consulta a la autoridad de seguridad de la Comisión, que el contrato o el acuerdo de subvención especifique los requisitos técnicos y administrativos necesarios relativos a la acreditación o aprobación del SIC en proporción al riesgo evaluado, teniendo en cuenta todos los factores pertinentes. El ámbito de la acreditación o aprobación de dicho SIC se determinará mediante acuerdo entre la autoridad de seguridad de la Comisión y la ANS o ASD correspondiente.

## CAPÍTULO 7

**INTERCAMBIO DE INFORMACIÓN CLASIFICADA CON OTRAS INSTITUCIONES, ÓRGANOS, ORGANISMOS Y OFICINAS DE LA UNIÓN, CON LOS ESTADOS MIEMBROS Y CON TERCEROS ESTADOS Y ORGANIZACIONES INTERNACIONALES***Artículo 51***Principios básicos**

1. En caso de que la Comisión o uno de sus servicios determine que existe la necesidad de intercambiar ICUE con otra institución, órgano, organismo u oficina de la Unión, o con un tercer Estado o una organización internacional, se tomarán las medidas necesarias para establecer un marco jurídico o administrativo adecuado a tal efecto, que podrá incluir acuerdos sobre seguridad de la información o acuerdos administrativos celebrados de conformidad con la normativa pertinente.
2. Sin perjuicio de lo dispuesto en el artículo 57, solo se podrá intercambiar ICUE con otra institución, órgano, organismo u oficina de la Unión, o con un tercer Estado o una organización internacional, siempre que esté vigente tal marco jurídico o administrativo adecuado, y que existan suficientes garantías de que la institución, órgano, organismo u oficina de la Unión, o el tercer Estado u organización internacional de que se trate aplica principios básicos y normas mínimas equivalentes para la protección de la información clasificada.

*Artículo 52***Intercambio de ICUE con otras instituciones, órganos, organismos y oficinas de la Unión**

1. Antes de celebrar un acuerdo administrativo para el intercambio de ICUE con otra institución, órgano, organismo u oficina de la Unión, la Comisión recabará garantías de que la institución, órgano u organismo de que se trate:
  - a) dispone de un marco reglamentario para la protección de la ICUE que establezca principios básicos y normas mínimas equivalentes a las previstas en la presente Decisión y sus normas de desarrollo;
  - b) aplica normas de seguridad y directrices en lo que respecta a la seguridad del personal, la seguridad física, la gestión de la seguridad de la ICUE y la seguridad de los sistemas de información y comunicaciones (SIC), que garanticen un nivel de protección de la ICUE equivalente al que se concede en la Comisión;
  - c) señale como ICUE la información clasificada que cree.
2. La Dirección General de Recursos Humanos y Seguridad, en estrecha cooperación con otros servicios competentes de la Comisión, será el servicio responsable de la Comisión para la celebración de acuerdos administrativos para el intercambio de ICUE con otras instituciones, órganos, organismos y agencias de la Unión.
3. Por regla general, los acuerdos administrativos adoptarán la forma de un canje de notas, firmado por el director general de Recursos Humanos y Seguridad en nombre de la Comisión.
4. Antes de celebrar un acuerdo administrativo de intercambio de ICUE, la autoridad de seguridad de la Comisión realizará una visita de evaluación destinada a evaluar el marco regulador para la protección de la ICUE y determinar la eficacia de las medidas establecidas para la protección de la ICUE. El acuerdo administrativo entrará en vigor, y se intercambiará ICUE, únicamente si los resultados de esta visita de evaluación son satisfactorios y se cumplen las recomendaciones formuladas a raíz de la visita. Se realizarán visitas de evaluación de seguimiento periódicas para comprobar que el acuerdo administrativo se cumple y que las medidas de seguridad establecidas siguen respetando los principios básicos y las normas mínimas acordadas.
5. Dentro de la Comisión, el registro de ICUE gestionado por la Secretaría General será, por regla general, el punto principal de entrada y salida para los intercambios de información clasificada con otras instituciones, órganos, organismos u oficinas de la Unión. No obstante, en caso de que, por razones de seguridad, de organización o de funcionamiento sea más adecuado para la protección de la ICUE, los registros locales de ICUE establecidos en los servicios de la Comisión de conformidad con la presente Decisión y sus normas de desarrollo funcionarán como punto de entrada y salida de la información clasificada con respecto a los asuntos que sean competencia de los servicios de la Comisión interesados.
6. El grupo de expertos de la Comisión en materia de seguridad será informado del proceso de celebración de acuerdos administrativos con arreglo a lo dispuesto en el apartado 2.



*Artículo 53***Intercambio de ICUE con los Estados miembros**

1. La ICUE podrá intercambiarse y cederse a los Estados miembros siempre que estos protejan dicha información con arreglo a los requisitos aplicables a la información clasificada que lleve una clasificación de seguridad nacional del nivel de clasificación equivalente según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el anexo I.
2. Cuando los Estados miembros introduzcan en las estructuras o redes de la Unión Europea información clasificada que lleve una marca nacional de clasificación de seguridad, la Comisión protegerá dicha información con arreglo a los requisitos aplicables a la ICUE del grado equivalente, según el cuadro de equivalencias de las clasificaciones de seguridad que figura en el anexo I.

*Artículo 54***Intercambio de ICUE con terceros Estados y organizaciones internacionales**

1. Cuando la Comisión determine que tiene la necesidad a largo plazo de intercambiar información clasificada con terceros Estados u organizaciones internacionales, se tomarán las medidas necesarias para establecer un marco jurídico o administrativo adecuado a tal efecto, que podrá incluir acuerdos sobre seguridad de la información o acuerdos administrativos celebrados de conformidad con la normativa pertinente.
2. Los acuerdos de seguridad de la información o los acuerdos administrativos a que se refiere el apartado 1 contendrán disposiciones que garanticen que los terceros países o las organizaciones internacionales que reciban ICUE protegerán dicha información de manera acorde con su grado de clasificación y conforme a normas mínimas que sean equivalentes a las que establece la presente Decisión.
3. La Comisión podrá celebrar acuerdos administrativos de conformidad con lo dispuesto en el artículo 56 cuando el nivel de clasificación de la ICUE no sea en general superior a RESTREINT UE/EU RESTRICTED.
4. Los acuerdos administrativos para el intercambio de información clasificada a que se refiere el apartado 3 contendrán disposiciones que garanticen que los terceros países o las organizaciones internacionales que reciban ICUE protegerán dicha información de manera acorde con su grado de clasificación y conforme a normas mínimas que no sean menos estrictas que las que establece la presente Decisión. El grupo de expertos de seguridad de la Comisión deberá ser consultado sobre la celebración de los acuerdos de seguridad de la información o acuerdos administrativos.
5. La decisión de ceder ICUE originada en la Comisión a un tercer Estado u organización internacional será adoptada por el servicio de la Comisión, como originador de la ICUE dentro de la Comisión, caso por caso, en función de la naturaleza y del contenido de dicha información, de la necesidad de conocer del destinatario y de la utilidad que pueda tener para la Unión. Si el originador de la información clasificada que se desea ceder, o del material fuente que contenga, no sea la Comisión, el servicio de la Comisión que posea esa información clasificada deberá recabar el consentimiento escrito del originador antes de comunicarla. En caso de que no sea posible determinar el originador, el servicio de la Comisión que tenga en su poder esa información clasificada asumirá la responsabilidad de aquel tras consultar al grupo de expertos de seguridad de la Comisión.

*Artículo 55***Acuerdos de seguridad de la información**

1. Los acuerdos de seguridad de la información con terceros Estados u organizaciones internacionales se celebrarán de conformidad con el artículo 218 del TFUE.
2. Los acuerdos de seguridad de la información:
  - a) establecerán los principios básicos y las normas mínimas aplicables al intercambio de información clasificada entre la Unión y un tercer Estado u organización internacional;
  - b) establecerán las disposiciones técnicas de aplicación que deban convenirse entre las autoridades de seguridad competentes de las instituciones y órganos pertinentes de la Unión y la autoridad de seguridad competente del tercer Estado u organización internacional de que se trate. Dichas disposiciones tendrán debidamente en cuenta el grado de protección que ofrezcan las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional de que se trate;
  - c) establecerán que, antes de intercambiarse la información clasificada en virtud del acuerdo, se comprobará que la parte receptora es capaz de proteger y salvaguardar la información clasificada que se le haya facilitado, de manera adecuada.

3. La Comisión consultará, cuando se determine una necesidad de intercambiar información clasificada de conformidad con el artículo 51, apartado 1, al Servicio Europeo de Acción Exterior, a la Secretaría General del Consejo y a otras instituciones y órganos de la Unión, según proceda, a fin de establecer si debe presentarse una recomendación de conformidad con el artículo 218, apartado 3, del TFUE.
4. No se intercambiará ICUE por medios electrónicos a menos que se haya previsto explícitamente en el acuerdo de seguridad de la información o en las disposiciones técnicas de aplicación.
5. Dentro de la Comisión, el registro de ICUE gestionado por la Secretaría General será, por regla general, el punto principal de entrada y salida para los intercambios de información clasificada con terceros Estados y organizaciones internacionales. No obstante, en caso de que, por razones de seguridad, de organización o de funcionamiento sea más adecuado para la protección de la ICUE, los registros locales de información clasificada establecidos en los servicios de la Comisión de conformidad con lo dispuesto en la presente Decisión y sus normas de desarrollo, funcionarán como punto de entrada y salida de la información clasificada con respecto a los asuntos que sean competencia de los servicios de la Comisión interesados.
6. Con el fin de evaluar la eficacia de las normas, estructuras y procedimientos de seguridad del tercer Estado o la organización internacional de que se trate, la Comisión, en colaboración con otras instituciones, órganos u organismos de la Unión, participará en visitas de evaluación de mutuo acuerdo con el tercer Estado o la organización internacional de que se trate. En dichas visitas se evaluará:
  - a) el marco regulador aplicable para proteger la información clasificada;
  - b) las características propias de la política de seguridad y la manera en que se organiza la seguridad en el tercer Estado u organización internacional, que pueden influir en el grado de la información clasificada que pueda intercambiarse;
  - c) las medidas y procedimientos de seguridad que se aplican efectivamente, y
  - d) los procedimientos de habilitación de seguridad del grado correspondiente al de la ICUE que ha de cederse.

#### Artículo 56

### Disposiciones administrativas

1. En los casos en que exista la necesidad a largo plazo, en el contexto de un marco político o jurídico de la Unión, de intercambiar información clasificada, en principio no superior al grado RESTREINT UE/EU RESTRICTED, con un tercer Estado o una organización internacional, y cuando la autoridad de seguridad de la Comisión, previa consulta al grupo de expertos de seguridad de la Comisión, haya establecido, en particular, que la parte en cuestión no cuenta con un sistema de seguridad suficientemente desarrollado como para que se pueda celebrar un acuerdo de seguridad de la información, la Comisión podría decidir celebrar un acuerdo administrativo con las autoridades competentes del tercer Estado o la organización internacional de que se trate.
2. Por regla general, tales acuerdos administrativos adoptarán la forma de un canje de notas.
3. Se realizará una visita de evaluación antes de la celebración del acuerdo. El grupo de expertos de seguridad de la Comisión será informado del resultado de la visita de evaluación. Cuando existan razones excepcionales para el intercambio urgente de información clasificada, podrá cederse la ICUE siempre que se haga todo lo posible para realizar una visita de evaluación cuanto antes.
4. No se intercambiará ICUE por medios electrónicos a menos que se haya establecido explícitamente en el acuerdo administrativo.

#### Artículo 57

### Cesión *ad hoc* con carácter excepcional de ICUE

1. En caso de que no exista un acuerdo de seguridad de la información o un acuerdo administrativo en vigor, y cuando la Comisión o uno de sus servicios determine que es necesario, a título excepcional, en el contexto de un marco jurídico o político de la Unión, ceder ICUE a un tercer Estado o a una organización internacional, la autoridad de seguridad de la Comisión comprobará, en la medida de lo posible, en colaboración con las autoridades de seguridad del tercer Estado u organización internacional de que se trate, que su normativa, estructuras y procedimientos de seguridad garantizan que la ICUE que se les ceda será protegida con arreglo a estándares no menos estrictos que los establecidos por la presente Decisión.
2. La decisión de ceder ICUE al tercer Estado u organización internacional de que se trate, previa consulta al grupo de expertos de seguridad de la Comisión, la tomará la Comisión sobre la base de una propuesta presentada por el miembro de la Comisión responsable de los asuntos de seguridad.

3. Una vez que haya tomado la Comisión la decisión de ceder ICUE, y con el consentimiento previo por escrito del originador, incluidos los originadores del material fuente que contenga, el servicio competente de la Comisión enviará el documento de que se trate, el cual deberá llevar una marca de posibilidad de cesión que indique a qué tercer Estado u organización internacional ha sido cedido. Antes o en el momento de la cesión efectiva, el tercero de que se trate se comprometerá por escrito a proteger la ICUE que reciba de acuerdo con los principios básicos y las normas mínimas que se establecen en la presente Decisión.

#### CAPÍTULO 8

#### DISPOSICIONES FINALES

##### Artículo 58

#### Sustitución de anteriores decisiones

La presente Decisión deroga y sustituye la Decisión 2001/844/CE, CECA, Euratom de la Comisión <sup>(1)</sup>.

##### Artículo 59

#### Información clasificada producida antes de la entrada en vigor de la presente Decisión

1. Toda la ICUE clasificada conforme a la Decisión 2001/844/CE, CECA, Euratom, seguirá estando protegida de acuerdo con las disposiciones pertinentes de la presente Decisión.
2. Toda la información clasificada en posesión de la Comisión en la fecha de entrada en vigor la Decisión 2001/844/CE, CECA, Euratom, con excepción de la información clasificada de Euratom:
  - a) en caso de proceder de la Comisión, se considerará que se ha reclasificado como «RESTREINT UE» por defecto, a no ser que su autor hubiese decidido darle otra clasificación antes del 31 de enero de 2002 y hubiese informado a todos los destinatarios del documento de que se trate;
  - b) en caso de que el autor sea ajeno a la Comisión, conservará su clasificación original y será tratada por consiguiente como ICUE de nivel equivalente, a no ser que el autor dé su consentimiento a la desclasificación o reducción del grado de clasificación de la información.

##### Artículo 60

#### Normas de desarrollo y consignas de seguridad

1. En caso necesario, la adopción de las normas de desarrollo de la presente Decisión será objeto de una nueva decisión de habilitación de la Comisión en favor del miembro de la Comisión responsable de las cuestiones de seguridad, de plena conformidad con el Reglamento interno.
2. Después de haber sido facultada a raíz de la Decisión de la Comisión anteriormente mencionada, el miembro de la Comisión responsable de las cuestiones de seguridad podrá elaborar consignas de seguridad que se establezcan directrices de seguridad y las mejores prácticas en el ámbito de aplicación de la presente Decisión y de las normas de desarrollo.
3. La Comisión podrá delegar las tareas mencionadas en los apartados 1 y 2 del presente artículo en el director general de la Dirección General de Recursos Humanos y Seguridad mediante una nueva decisión de delegación, de conformidad con el Reglamento interno.

##### Artículo 61

#### Entrada en vigor

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 13 de marzo de 2015.

Por la Comisión  
El Presidente  
Jean-Claude JUNCKER

<sup>(1)</sup> Decisión 2001/844/CE, CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno (DO L 317 de 3.12.2001, p. 1).

## ANEXO I

## EQUIVALENCIA DE LAS CLASIFICACIONES DE SEGURIDAD

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Bélgica	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	véase la nota (1)
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
República Checa	Prísne tajné	Tajné	Důvěrné	Vyhrazené
Dinamarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Alemania	Streng geheim	Geheim	VS (?) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
España	Secreto	Reservado	Confidencial	Difusión Limitada
Francia	Très Secret Défense	Secret Défense	Confidentiel Défense	véase la nota (2)
Croacia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Chipre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Letonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungría	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Países Bajos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Rumanía	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Eslovenia	Strogo tajno	Tajno	Zaupno	Interno
Eslovaquia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suecia (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Reino Unido	UK TOP SECRET	UK SECRET	No hay equivalente (5)	UK OFFICIAL-SENSITIVE

(1) Diffusion Restreinte/Beperkte Verspreiding no es una clasificación de seguridad en Bélgica. Bélgica maneja y protege la información «RESTREINT UE/EU RESTRICTED» de forma no menos rigurosa que las normas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

(2) Alemania: VS = Verschlussache.

(3) Francia no utiliza la clasificación «RESTREINT» en su sistema nacional. Francia maneja y protege la información «RESTREINT UE/EU RESTRICTED» de forma no menos rigurosa que las normas y procedimientos descritos en las normas de seguridad del Consejo de la Unión Europea.

(4) Suecia: Las marcas de clasificación de seguridad indicadas en la línea superior son las utilizadas por las autoridades de defensa, y las indicadas en la línea inferior las utilizadas por otras autoridades.

(5) El Reino Unido maneja y protege la ICUE señalada como CONFIDENTIEL UE/EU CONFIDENTIAL con arreglo a los requisitos de protección de seguridad correspondientes a «UK SECRET».

## ANEXO II

## LISTA DE ABREVIATURAS

Acrónimo	Significado
AAS	Autoridad de Acreditación de Seguridad
ACC	Autoridad de Certificación Criptológica
ADA	Autoridad debidamente acreditada
ADC	Autoridad de Distribución Criptológica
AGI	Autoridad de Garantía de la Información
ANS	Autoridad Nacional de Seguridad
ASD	Autoridad de Seguridad Designada
CCTV	Circuito cerrado de televisión
CHPS	Certificado de habilitación personal de seguridad
Coreper	Comité de Representantes Permanentes
ECSD	Dirección de Seguridad de la Comisión Europea
GI	Garantía de la Información
HPS	Habilitación personal de seguridad
ICUE	Información clasificada de la UE
PCSD	Política Común de Seguridad y Defensa
PESC	Política Exterior y de Seguridad Común
REUE	Representante Especial de la UE
SDI	Sistema de detección de intrusiones
SGC	Secretaría General del Consejo
SIC	Sistemas de información y comunicaciones que manejan ICUE
TI	Tecnologías de la información
TFUE	Tratado de Funcionamiento de la Unión Europea

## ANEXO III

## LISTA DE AUTORIDADES NACIONALES DE SEGURIDAD

## BÉLGICA

Autorité nationale de Sécurité  
 SPF Affaires étrangères, Commerce extérieur et  
 Coopération au Développement  
 15, rue des Petits Carmes  
 1000 Bruxelles  
 Tel. Secretariat: +32 25014542  
 Fax +32 25014596  
 Correo electrónico: nvo-ans@diplobel.fed.be

## BULGARIA

State Commission on Information Security  
 90 Cherkovna Str.  
 1505 Sofia  
 Tel. +359 29333600  
 Fax +359 29873750  
 Correo electrónico: dksi@government.bg  
 Website: www.dksi.bg

## REPÚBLICA CHECA

Národní bezpečnostní úřad  
 (National Security Authority)  
 Na Popelce 2/16  
 150 06 Praha 56  
 Tel. +420 257283335  
 Fax +420 257283110  
 Correo electrónico: czech.nsa@nbu.cz  
 Website: www.nbu.cz

## DINAMARCA

Politiets Efterretningstjeneste  
 (Danish Security Intelligence Service)  
 Klausdalsbrovej 1  
 2860 Søborg  
 Tel. +45 33148888  
 Fax +45 33430190  
 Forsvarets Efterretningstjeneste  
 (Danish Defence Intelligence Service)  
 Kastellet 30  
 2100 Copenhagen Ø  
 Tel. +45 33325566  
 Fax +45 33931320

## ALEMANIA

Bundesministerium des Innern  
 Referat ÖS III 3  
 Alt-Moabit 101 D  
 D-11014 Berlin  
 Tel. +49 30186810  
 Fax +49 30186811441  
 Correo electrónico: oesIII3@bmi.bund.de

## ESTONIA

National Security Authority Department  
 Estonian Ministry of Defence  
 Sakala 1  
 15094 Tallinn  
 Tel. +372 7170113 0019, +372 7170117  
 Fax +372 7170213  
 Correo electrónico: nsa@mod.gov.ee

## GRECIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)  
 Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)  
 Διεύθυνση Ασφαλείας και Αντιπληροφοριών  
 ΣΤΤ 1020 -Χολαργός (Αθήνα)  
 Ελλάδα  
 Τηλ.: +30 2106572045 (ώρες γραφείου)  
 + 30 2106572009 (ώρες γραφείου)  
 Φαξ: +30 2106536279; + 30 2106577612  
 Hellenic National Defence General Staff (HNDGS)  
 Military Intelligence Sectoral Directorate  
 Security Counterintelligence Directorate  
 GR-STG 1020 Holargos — Athens  
 Tel. +30 2106572045  
 + 30 2106572009  
 Fax +30 2106536279, +30 2106577612

## ESPAÑA

Autoridad Nacional de Seguridad  
 Oficina Nacional de Seguridad  
 Avenida Padre Huidobro s/n  
 28023 Madrid  
 Tel. +34 913725000  
 Fax +34 913725808  
 Correo electrónico: nsa-sp@areatec.com

## FRANCIA

Secrétariat général de la défense et de la sécurité nationale

Sous-direction Protection du secret (SGDSN/PSD)

51 Boulevard de la Tour-Maubourg

75700 Paris 07 SP

Tel. +33 171758177

Fax + 33 171758200

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

4 Emanuel Roidi street

1432 Nicosia

Tel. +357 22807569, +357 22807643,

+357 22807764

Fax +357 22302351

Correo electrónico: cynsa@mod.gov.cy

## CROACIA

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagreb

Croatia

Tel. +385 14681222

Fax + 385 14686049

Website: www.uvns.hr

## LETONIA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O.Box 286

LV-1001 Riga

Tel. +371 67025418

Fax +371 67025454

Correo electrónico: ndi@sab.gov.lv

## IRLANDA

National Security Authority

Department of Foreign Affairs

76-78 Harcourt Street

Dublin 2

Tel. +353 14780822

Fax +353 14082959

## LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)

Gedimino 40/1

LT-01110 Vilnius

Tel. +370 706 66701, +370 706 66702

Fax +370 706 66700

Correo electrónico: nsa@vsd.lt

## ITALIA

Presidenza del Consiglio dei Ministri

D.I.S.-U.C.Se.

Via di Santa Susanna, 15

00187 Roma

Tel. +39 0661174266

Fax +39 064885273

## LUXEMBURGO

Autorité nationale de Sécurité

Boîte postale 2379

1023 Luxembourg

Tel. +352 24782210 central

+ 352 24782253 direct

Fax +352 24782243

## CHIPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,

+357 22807764

Τηλεμοιότυπο: +357 22302351

## HUNGRÍA

Nemzeti Biztonsági Felügyelet

(National Security Authority of Hungary)

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel. +36 (1) 7952303

Fax +36 (1) 7950344

Postal address:

H-1357 Budapest, PO Box 2

Correo electrónico: nbf@nbf.hu

Website: www.nbf.hu



## MALTA

Ministry for Home Affairs and National Security  
P.O. Box 146  
MT-Valletta  
Tel. +356 21249844  
Fax +356 25695321

1300-342 Lisboa  
Tel. +351 213031710  
Fax +351 213031711

## PAÍSES BAJOS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
Postbus 20010  
2500 EA Den Haag  
Tel. +31 703204400  
Fax +31 703200733  
Ministerie van Defensie  
Beveiligingsautoriteit  
Postbus 20701  
2500 ES Den Haag  
Tel. +31 703187060  
Fax +31 703187522

## RUMANÍA

Oficiul Registrului Național al Informațiilor Secrete de Stat  
(Romanian NSA — ORNISS National Registry Office for Classified Information)  
4 Mures Street  
012275 Bucharest  
Tel. +40 212245830  
Fax +40 212240714  
Correo electrónico: nsa.romania@nsa.ro  
Website: www.orniss.ro

## AUSTRIA

Informationssicherheitskommission  
Bundeskanzleramt  
Ballhausplatz 2  
1014 Wien  
Tel. +43 1531152594  
Fax +43 1531152615  
Correo electrónico: ISK@bka.gv.at

## ESLOVENIA

Urad Vlade RS za varovanje tajnih podatkov  
Gregorčičeva 27  
1000 Ljubljana  
Tel. +386 14781390  
Fax +386 14781399  
Correo electrónico: gp.uvtp@gov.si

## POLONIA

Agencja Bezpieczeństwa Wewnętrznego — ABW  
(Internal Security Agency)  
2A Rakowiecka St.  
00-993 Warszawa  
Tel. +48 22 58 57 944  
fax +48 22 58 57 443  
Correo electrónico: nsa@abw.gov.pl  
Website: www.abw.gov.pl

## ESLOVAQUIA

Národný bezpečnostný úrad  
(National Security Authority)  
Budatínska 30  
P.O. Box 16  
850 07 Bratislava  
Tel. +421 268692314  
Fax +421 263824005  
Website: www.nbusr.sk

## PORTUGAL

Presidência do Conselho de Ministros  
Autoridade Nacional de Segurança  
Rua da Junqueira, 69

## FINLANDIA

National Security Authority  
Ministry for Foreign Affairs  
P.O. Box 453  
FI-00023 Government  
Tel. 16055890  
Fax +358 916055140  
Correo electrónico: NSA@formin.fi

SUECIA

Utrikesdepartementet

(Ministry for Foreign Affairs)

SSSB

S-103 39 Stockholm

Tel. +46 84051000

Fax +46 87231176

Correo electrónico: [ud-nsa@foreign.ministry.se](mailto:ud-nsa@foreign.ministry.se)

REINO UNIDO

UK National Security Authority

Room 335, 3rd Floor

70 Whitehall

London

SW1A 2AS

Tel. 1: +44 2072765649

Tel. 2: +44 2072765497

Fax +44 2072765651

Correo electrónico: [UK-NSA@cabinet-office.x.gsi.gov.uk](mailto:UK-NSA@cabinet-office.x.gsi.gov.uk)

---



ISSN 1977-0685 (edición electrónica)  
ISSN 1725-2512 (edición papel)



**Oficina de Publicaciones de la Unión Europea**  
2985 Luxemburgo  
LUXEMBURGO

**ES**