

No. 57573*

**Spain
and
Peru**

Agreement between the Kingdom of Spain and the Republic of Peru for the exchange and reciprocal protection of classified information in the field of defence. Madrid, 28 February 2019

Entry into force: *3 December 2022, in accordance with article 16(1)*

Authentic text: *Spanish*

Registration with the Secretariat of the United Nations: *Spain, 3 December 2022*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

**Espagne
et
Pérou**

Accord entre le Royaume d'Espagne et la République du Pérou relatif à l'échange et la protection réciproque des informations classifiées dans le domaine de la défense. Madrid, 28 février 2019

Entrée en vigueur : *3 décembre 2022, conformément au paragraphe 1 de l'article 16*

Texte authentique : *espagnol*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Espagne, 3 décembre 2022*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[TEXT IN SPANISH – TEXTE EN ESPAGNOL]

ACUERDO

ENTRE

EL REINO DE ESPAÑA

Y

LA REPÚBLICA DEL PERÚ

PARA EL INTERCAMBIO Y PROTECCIÓN RECÍPROCA

DE INFORMACIÓN CLASIFICADA

EN EL ÁMBITO DE LA DEFENSA

El Reino de España y la República del Perú

En lo sucesivo denominados las “Partes”

Manifestando el deseo de garantizar la protección de la Información Clasificada, cuyo intercambio se materialice o genere en el ámbito de la defensa,

Teniendo en consideración el interés mutuo de garantizar la protección de la Información Clasificada en dicho ámbito, en concordancia con las leyes y reglamentos nacionales de las Partes.

Han convenido en lo siguiente:

ARTICULO 1 ÁMBITO DE APLICACIÓN

El presente Acuerdo establece las reglas y procedimientos para la protección de la Información Clasificada en el ámbito de la defensa, intercambiada o generada entre las Partes, sus personas físicas, órganos o entidades acreditadas.

ARTICULO 2 OBLIGACIONES GENERALES

1. Ambas Partes deberán adoptar todas las medidas que sean necesarias para asegurar la protección de la Información Clasificada transmitida o generada al amparo del presente Acuerdo, en conformidad con sus leyes y reglamentos nacionales.
2. Ninguna de las Partes podrá invocar el presente Acuerdo con el fin de obtener Información Clasificada que la otra Parte haya recibido de una Tercera Parte.

ARTICULO 3 DERECHOS DE PROPIEDAD INTELECTUAL

1. La protección de la propiedad intelectual estará regulada por las legislaciones nacionales respectivas de las Partes y los acuerdos internacionales sobre la materia que sean aplicable a ambas Partes.

2. Nada de lo dispuesto en el presente Acuerdo podrá reducir ni limitar ningún derecho de propiedad intelectual asociado a la Información Clasificada intercambiada del que sea titular una de las Partes, sus contratistas o cualquier tercero.
3. Los derechos de propiedad intelectual de la Información Clasificada generada al amparo del presente Acuerdo serán definidos por las Partes, en conformidad con sus respectivas leyes y reglamentos nacionales.

ARTICULO 4 DEFINICIONES

A los efectos del presente Acuerdo:

- a) Por "**Información Clasificada**" se entenderá cualquier dato, con independencia de su forma, naturaleza o método de transmisión, que requiera protección contra su divulgación no autorizada o su pérdida, y a la que se haya asignado una clasificación de seguridad de conformidad con las leyes y reglamentos nacionales de las Partes.
- b) Por "**Portadores de Información Clasificada**" se entenderá los objetos materiales en los cuales la Información Clasificada se refleja en modo de símbolos, imágenes, señales, resoluciones técnicas y procesos. Su protección se rige por la legislación nacional de cada Parte.
- c) Por "**Autoridad Competente**" se entenderá la autoridad designada por cada Parte para la aplicación y supervisión del presente Acuerdo, conforme a lo señalado en el Artículo 5;
- d) Por "**Parte de Origen**" se entenderá la Parte que ceda Información Clasificada;
- e) Por "**Parte Receptora**" se entenderá aquella que reciba la Información Clasificada transmitida por la Parte de Origen;
- f) Por "**Tercera Parte**" se entenderá cualquier organización internacional o Estado que no sea Parte en el presente Acuerdo;
- g) Por "**Instrucciones de Seguridad**" se entenderá el conjunto de procedimientos y medidas de seguridad adicionales para proteger la Información Clasificada, establecidas en un determinado Contrato Clasificado.

- h) Por "**Contrato Clasificado**" se entenderá cualquier contrato, convenio o acuerdo de cooperación cuyo objeto o ejecución implique el acceso o manejo de Información Clasificada, entendiéndose por tal la generación, tratamiento o almacenamiento de dicha información, en el marco del presente Acuerdo;
- i) Por "**Subcontrato Clasificado**" se entenderá cualquier contrato, convenio o acuerdo derivado del Contrato Clasificado cuyo objeto o ejecución implique el acceso o manejo de Información Clasificada, entendiéndose por tal la generación, tratamiento o almacenamiento de dicha información, en el marco del presente Acuerdo;
- j) Por "**Contratista o Subcontratista**" se entenderá la entidad jurídica o persona, acreditada por la autoridad Competente, con capacidad para celebrar un Contrato Clasificado en los términos previstos en el presente Acuerdo y conforme a las leyes y reglamentos nacionales de las Partes;
- k) Por "**Comprometimiento de Seguridad**" se entenderá cualquier acto u omisión, intencional o accidental, del que resulte la puesta en peligro o el riesgo que ponga en peligro la Información Clasificada;
- l) Por "**Habilitación Personal de Seguridad**" se entenderá la determinación por parte de la Autoridad Competente de que una persona cumple los requisitos para tener acceso a la Información Clasificada, de conformidad con sus respectivas leyes y reglamentos nacionales;
- m) Por "**Habilitación de Seguridad de Establecimiento**" se entenderá la determinación por parte de la Autoridad Competente de que un establecimiento posee, desde el punto de vista de la seguridad, la capacidad material y organizativa para generar, almacenar y gestionar Información Clasificada, de conformidad con las respectivas leyes y reglamentos nacionales; y
- n) Por "**Necesidad de Conocer**" se entenderá el principio conforme al cual sólo se permitirá acceder a la Información Clasificada a una persona que tenga la necesidad acreditada de hacerlo en relación con sus funciones oficiales, en el marco de las cuales se cedió dicha información a la Parte Receptora;

ARTICULO 5
AUTORIDADES COMPETENTES

1. Las Autoridades Competentes responsables de la aplicación del presente acuerdo son:

Por el Reino de España:

Secretario de Estado, Director del Centro Nacional de Inteligencia,
o su representante
Oficina Nacional de Seguridad

Por la República del Perú:

Ministro de Defensa o su representante

2. Ambas autoridades, cada una dentro del territorio de su país, velarán por la protección de la Información Clasificada transmitida de conformidad con sus leyes y reglamentos nacionales y las disposiciones del presente Acuerdo.
3. A fin de alcanzar y mantener niveles comparables de seguridad, las Autoridades Competentes, previa solicitud, se facilitarán mutuamente información sobre su legislación, normativa, organización y procedimientos de seguridad y permitirán las visitas a su territorio de representantes debidamente acreditados de la otra Parte.
4. Previa solicitud, las Partes, a través de sus Autoridades Competentes, y teniendo en cuenta sus respectivas legislaciones nacionales, colaborarán mutuamente durante los procedimientos necesarios para la habilitación de seguridad de sus ciudadanos residentes o que hayan residido en el territorio de la otra Parte.
5. Las Autoridades Competentes adoptarán las medidas pertinentes para que las personas físicas, órganos o entidades habilitadas de su país cumplan las obligaciones del presente Acuerdo.

ARTICULO 6
CLASIFICACIÓN DE SEGURIDAD

1. Las Partes acuerdan la siguiente equivalencia entre los grados de clasificación:

Reino de España	República del Perú
RESERVADO	SECRETO
CONFIDENCIAL	RESERVADO
DIFUSIÓN LIMITADA	CONFIDENCIAL

2. La Parte Receptora concederá a la Información Clasificada recibida el grado de clasificación equivalente al asignado por la Parte de Origen, de conformidad con lo dispuesto en el párrafo precedente.
3. La Parte Receptora no podrá reclasificar o desclasificar la Información Clasificada recibida sin la previa autorización escrita de la Autoridad Competente de la Parte de Origen.
4. La Parte de Origen informará a la Parte Receptora de la reclasificación o desclasificación de la Información Clasificada transmitida.

ARTICULO 7
MANEJO DE LA INFORMACIÓN CLASIFICADA

1. Nadie estará autorizado a acceder a la Información Clasificada únicamente por razón de su rango o nombramiento o por poseer una Habilitación Personal de Seguridad. El acceso de la Información Clasificada se otorgará sólo a aquellas personas con Necesidad de Conocer que hayan obtenido la habilitación pertinente y la correspondiente autorización para acceder a la misma, de conformidad con las leyes y reglamentos nacionales de la Parte respectiva.
2. Las Partes aceptarán la Habilitación Personal de Seguridad emitida por la Autoridad Competente de la otra Parte.

3. Previa solicitud, las Partes, a través de sus Autoridades Competentes, y teniendo en cuenta sus respectivas leyes y reglamentos nacionales, se prestarán mutua asistencia en la aplicación de los procedimientos de habilitación referentes a las Habilitaciones Personales de Seguridad y/o las Habilitaciones de Seguridad de Establecimiento. Las Autoridades Competentes de ambas Partes podrán acordar mecanismos específicos a tal fin.
4. La Información Clasificada intercambiada solo podrá utilizarse para los fines para los que fue transmitida.

ARTICULO 8 TRADUCCIÓN, REPRODUCCIÓN Y DESTRUCCIÓN DE LA INFORMACIÓN CLASIFICADA

1. Las traducciones y reproducciones de la Información Clasificada se realizarán con arreglo a los siguientes procedimientos:
 - a) Sólo podrán realizar traducciones y reproducciones de Información Clasificada las personas que cuenten con la autorización correspondiente, y que sean titulares de una Habilitación Personal de Seguridad del grado de clasificación de seguridad de la Información Clasificada que se reproduzca o traduzca;
 - b) El número de copias se limitará al requerido para fines oficiales;
 - c) Las copias deberán estar marcadas con la misma clasificación que la Información Clasificada original y deberán ser controladas por las Partes; y
 - d) La Información Clasificada de grado RESERVADO para la Parte española y SECRETO para la Parte peruana sólo podrá reproducirse cuando la Autoridad Competente de la Parte Receptora haya recibido la autorización escrita de la Autoridad Competente de la Parte de Origen.
2. La destrucción de la Información Clasificada se llevará a cabo conforme a las leyes y reglamentos nacionales de la Parte Receptora cuando ya no se considere necesaria, de modo que se impida su reconstrucción o reconocimiento total o parcial.

3. La Información Clasificada de grado RESERVADO para la Parte española y SECRETO para la Parte peruana solo se destruirá previo consentimiento escrito de la Parte de Origen.

ARTICULO 9 TRANSMISIÓN DE LA INFORMACIÓN CLASIFICADA

1. La Información Clasificada se transmitirá entre las Partes por conducto diplomático, o a través de personas físicas, órganos o entidades debidamente habilitados y autorizados por la Parte de Origen y según los procedimientos mutuamente acordados entre las Autoridades Competentes de las Partes.
2. La Información Clasificada solo podrá transmitirse a través de sistemas de comunicaciones protegidos, redes u otros medios electromagnéticos aprobados y autorizados por las Autoridades Competentes de ambas Partes.
3. La transmisión de Información Clasificada voluminosa o en grandes cantidades será aprobada, en cada caso, por ambas Autoridades Competentes.
4. La Autoridad Competente de la Parte Receptora confirmará, por escrito, la recepción de la Información Clasificada.
5. La Parte Receptora no transmitirá Información Clasificada a ninguna Tercera Parte ni a personas físicas, órgano o entidad alguna que tenga la nacionalidad de un tercer Estado, sin previa autorización escrita de la Parte de Origen.

ARTICULO 10 PORTADORES DE INFORMACIÓN CLASIFICADA

1. Los Portadores de Información Clasificada recibida serán marcados por la entidad receptora con el grado de clasificación equivalente, en conformidad con el Artículo 6 del presente Acuerdo.
2. La obligación de marcar con los grados de clasificación equivalentes establecidos se extenderá a los Portadores de la Información Clasificada generada en el proceso de cooperación conjunta de las Partes, así como la generada como resultado de la realización de traducciones o reproducciones.

3. El proceso de destrucción de los Portadores de Información Clasificada se realizará de conformidad con la legislación nacional de la Parte Receptora cuando ya no se consideren necesarios, previa autorización de la Parte de Origen. La destrucción deberá garantizar la imposibilidad de la recuperación o reproducción total o parcial de la Información Clasificada.
4. Las demás especificaciones relativas al tratamiento de los Portadores de Información Clasificada, se realizarán de conformidad con las leyes y reglamentos nacionales de las Partes.

ARTICULO 11 CONTRATOS CLASIFICADOS

1. La Parte que desee adjudicar un Contrato Clasificado a un Contratista de la otra Parte o que uno de sus propios Contratistas concluya un Contrato Clasificado en el territorio de la otra Parte, deberá obtener previamente una garantía por escrito de la Autoridad Competente de la otra Parte de que el Contratista propuesto posee una Habilidad de Seguridad de Establecimiento del grado apropiado.
2. De acuerdo al párrafo precedente, todo Subcontratista deberá también estar habilitado, comprometiéndose a proteger la Información Clasificada, de conformidad con lo dispuesto en el párrafo 5 del presente Artículo.
3. Los Contratos Clasificados se celebrarán y aplicarán de conformidad con las leyes y reglamentos nacionales de cada Parte.
4. Se incluirá en cada Contrato Clasificado o subcontrato, formando parte integrante del mismo, un anexo de seguridad sobre protección de la Información Clasificada, que contemple los siguientes aspectos:
 - a) Identificación de la Información Clasificada;
 - b) Instrucciones de Seguridad del proyecto que definan el conjunto de procedimientos y medidas de seguridad aplicables a la Información Clasificada;
 - c) Responsabilidades por los daños derivados de cualquier Comprometimiento de Seguridad.
 - d) Obligación de informar de cualquier Comprometimiento de Seguridad a la Autoridad Competente correspondiente;

- e) Previsión de los canales de comunicación o de los medios para la transmisión de la Información Clasificada;
 - f) Obligación de que el Contratista, sus empleados, directivos o representantes mantengan la confidencialidad correspondiente; y
 - g) Responsabilidades por el incumplimiento de los procedimientos y medidas de seguridad aplicables a la Información Clasificada.
5. La responsabilidad del Contratista de proteger la Información Clasificada comprenderá, como mínimo, la obligación de:
- a) Dar acceso a la Información Clasificada sólo a las personas que cuenten con la Habilitación Personal de Seguridad y tengan Necesidad de Conocer;
 - b) Articular los medios necesarios para transmitir Información Clasificada de forma segura;
 - c) Establecer los procedimientos para las visitas del personal de una de las Partes a la otra;
 - d) Informar a su Autoridad Competente de cualquier acceso, intento de acceso o sospecha de acceso no autorizado a la Información Clasificada intercambiada;
 - e) Utilizar la Información Clasificada recibida sólo para los fines para los cuales fue transmitida; y
 - f) Cumplir los procedimientos establecidos por las leyes y reglamentos respectivos en relación con el manejo de la Información Clasificada, conforme a las legislaciones nacionales de las Partes y a las disposiciones de este Acuerdo.
6. Deberá remitirse una copia de cada Contrato Clasificado o Subcontrato a la Autoridad Competente de la Parte en cuyo territorio vaya a ejecutarse el Contrato Clasificado o Subcontrato, con el fin de verificar el cumplimiento de las cláusulas de seguridad.
7. Cuando se produzca cualquier hecho que haga innecesaria la retención de la Información Clasificada transmitida, toda la Información Clasificada intercambiada o generada al amparo de un Contrato Clasificado se destruirá, de conformidad con las leyes y reglamentos nacionales de la Parte Receptora.

ARTICULO 12 VISITAS

1. Las visitas de nacionales de una Parte a la otra Parte, que impliquen acceso a la Información Clasificada, estarán sujetas a autorización previa, por escrito, de la Autoridad Competente de la Parte anfitriona, y se realizará de conformidad con las leyes y reglamentos nacionales de dicha Parte.
2. La solicitud de visita se presentará a través de las Autoridades Competentes con una antelación mínima de veinte (20) días respecto a la fecha prevista para la visita.
3. Cada Parte autorizará las visitas de la otra Parte únicamente cuando los visitantes:
 - a) Estén en posesión de una Habilitación Personal de Seguridad válida concedida por su país de origen; y
 - b) Estén autorizados a recibir o tener acceso a Información Clasificada en virtud de una Necesidad de Conocer.
4. La solicitud de visita se presentará a través de la Autoridad Competente, debiendo incluir la siguiente información:
 - a) Datos personales del visitante: nombre y apellidos, fecha y lugar de nacimiento, nacionalidad, número de pasaporte u otro documento de identidad;
 - b) Indicación del órgano o entidad al que pertenece el visitante;
 - c) Datos relacionados con la visita: periodo de la visita, objeto y propósito de la misma, indicación de la entidad o entidades que se desea visitar;
 - d) Indicación de un punto de contacto en el órgano o entidad que se desea visitar, con nombres, apellidos y número de teléfono y/o correo electrónico;
 - e) Indicación del nivel de clasificación de información a la que se desea acceder; y

- f) Certificación de la tenencia de una Habilitación de Seguridad del visitante, en la que figure el nivel de clasificación, el plazo de validez y cualquier limitación que conste en la misma;
- 5. La Autoridad Competente del país anfitrión notificará su decisión a la Autoridad Competente del país del visitante con una antelación mínima de diez (10) días respecto a la fecha prevista para la visita.
- 6. Una vez que haya sido autorizada la visita, la Autoridad Competente de la Parte anfitriona remitirá una copia de la solicitud de visita a la entidad que vaya a ser visitada. Esta última deberá informar al visitante de las reglamentaciones y procedimientos correspondientes que deberán acatarse durante la visita.
- 7. Todos los visitantes deberán cumplir con las reglamentaciones de seguridad y procedimientos para el acceso a las instalaciones a visitar. Los visitantes no divulgarán a terceros no autorizados la Información Clasificada a la que tuvieron acceso durante su visita.
- 8. En caso de Contratos Clasificados que exijan visitas periódicas, las Partes podrán elaborar listas de personas autorizadas. Dichas listas no podrán tener una validez superior a doce (12) meses.
- 9. Cada Parte protegerá los datos personales de los visitantes, de conformidad con las leyes y reglamentos nacionales aplicables.

ARTICULO 13 COMPROMETIMIENTO DE SEGURIDAD

- 1. En el caso de Comprometimiento de Seguridad relacionada con la Información Clasificada, la Autoridad Competente de la Parte donde se haya producido el Comprometimiento de Seguridad informará inmediatamente a la Autoridad Competente de la otra Parte.
- 2. La Parte donde se haya producido el Comprometimiento de Seguridad deberá investigar o colaborar en la investigación del incidente e informar tan pronto como sea posible a la otra Parte sobre el resultado de la investigación y las medidas correctivas aplicables.

**ARTICULO 14
GASTOS**

1. El presente Acuerdo no prevé la generación de gasto alguno.
2. Si se produce algún gasto, cada Parte sufragará sus propios gastos derivados de la aplicación y supervisión de todos los aspectos del presente Acuerdo, de conformidad con sus leyes y reglamentos nacionales.

**ARTICULO 15
SOLUCIÓN DE CONTROVERSIAS**

1. Cualquier controversia sobre la interpretación o aplicación del presente Acuerdo se resolverá mediante consultas entre las Partes por la vía diplomática.
2. Las Partes continuarán cumpliendo con las obligaciones que derivan del presente Acuerdo durante el período de solución de las controversias con arreglo al párrafo anterior.

**ARTICULO 16
DISPOSICIONES FINALES**

1. El presente Acuerdo entrará en vigor a los treinta (30) días de la fecha de recepción de la última de las notificaciones escritas intercambiadas por las Partes, por la vía diplomática, en las que se comunique el cumplimiento de los procedimientos exigidos por sus respectivos ordenamientos jurídicos para tal efecto, y tendrá una duración indefinida.
2. El presente Acuerdo podrá enmendarse con el consentimiento mutuo, por escrito, de ambas Partes. Las enmiendas entrarán en vigor con arreglo a lo dispuesto en el párrafo precedente.
3. Cualquiera de las Partes podrá denunciar el presente Acuerdo mediante notificación escrita a la otra Parte, por la vía diplomática. La denuncia surtirá efectos a los seis (6) meses de recibida la notificación por la otra Parte.

4. No obstante la denuncia, toda la Información Clasificada transmitida en virtud del presente Acuerdo seguirá protegida conforme a las disposiciones establecidas en el mismo, hasta que la Parte de Origen elimine la clasificación o decida o autorice su destrucción.

Firmado el presente Acuerdo en Madrid, el 28 de febrero de 2019, en dos ejemplares, siendo ambos igualmente auténticos.

Por el Reino de España



PEDRO SÁNCHEZ PÉREZ-CASTEJÓN
Presidente de España

Por la República del Perú



MARTÍN VIZCARRA CORNEJO
Presidente del Perú

[TRANSLATION – TRADUCTION]

AGREEMENT BETWEEN THE KINGDOM OF SPAIN AND THE REPUBLIC OF PERU FOR THE EXCHANGE AND RECIPROCAL PROTECTION OF CLASSIFIED INFORMATION IN THE FIELD OF DEFENCE

The Kingdom of Spain and the Republic of Peru,
hereinafter referred to as the “Parties”,

Expressing their desire to protect classified information exchanged or generated in the area of defence,

Bearing in mind their mutual interest in protecting such classified information, in accordance with the national laws and regulations of the Parties,

Have agreed as follows:

Article 1. Scope

This Agreement establishes the rules and procedures for the protection of classified information in the field of defence, exchanged or generated between the Parties, their natural persons, organs or accredited entities.

Article 2. General obligations

1. Both Parties shall take all necessary measures to ensure the protection of classified information transmitted or generated under this Agreement, in accordance with their national laws and regulations.

2. This Agreement may not be invoked by either Party in order to obtain classified information that the other Party has received from a third party.

Article 3. Intellectual property rights

1. The protection of intellectual property shall be regulated by the respective national laws of the Parties and the relevant international agreements applicable to both Parties.

2. Nothing in this Agreement shall reduce or restrict any intellectual property rights associated with the exchanged classified information owned by either Party, its contractors or any third party.

3. The intellectual property rights to classified information generated under this Agreement shall be defined by the Parties, in accordance with their respective national laws and regulations.

Article 4. Definitions

For the purposes of this Agreement:

- (a) “Classified information” means any information, regardless of its form, nature or method of transmission, that requires protection against unauthorized disclosure or

loss, and which has been assigned a security classification in accordance with the national laws and regulations of the Parties.

- (b) “Classified information carriers” means material objects on which classified information is reflected in the form of symbols, images, signs, technical resolutions and processes. Their protection is governed by the national law of each Party.
 - (c) “Competent authority” means the authority designated by each Party to implement and monitor this Agreement, in accordance with article 5;
 - (d) “Originating Party” means the Party that releases classified information;
 - (e) “Receiving Party” means the Party that receives classified information from the Originating Party;
 - (f) “Third party” means any international organization or State that is not a Party to this Agreement;
 - (g) “Security instructions” means the set of additional security procedures and measures to protect classified information set forth in a particular classified contract.
 - (h) “Classified contract” means any cooperation contract, arrangement or agreement the purpose or implementation of which entails access to or handling of classified information, understood as the generation, processing or storage of such information under this Agreement;
 - (i) “Classified subcontract” means any contract, agreement or arrangement derived from the classified contract, the purpose or implementation of which entails access to or handling of classified information, understood as the generation, processing or storage of such information under this Agreement;
 - (j) “Contractor or subcontractor” means the legal entity or person, accredited by the competent authority, with the capacity to enter into a classified contract under the terms of this Agreement and in accordance with the national laws and regulations of the Parties;
 - (k) “Security breach” means any act or omission, intentional or accidental, which either endangers or risks endangering classified information;
- (1) “Personal security clearance” means the determination by the competent authority that a person meets the requirements to have access to classified information, in accordance with their respective national laws and regulations;
- (m) “Facility security clearance” means a determination by the competent authority that, from a security standpoint, a facility has the physical and organizational capability to generate, store and handle classified information, in accordance with the respective national laws and regulations; and
 - (n) “Need to know” means the principle that access to classified information shall be granted only to a person who has a demonstrated need of such access in connection with his or her official duties, in the context of which the information was disclosed to the Receiving Party;

Article 5. Competent authorities

1. The competent authorities responsible for the implementation of this Agreement are:

For the Kingdom of Spain:

Secretary of State, Director of the National Intelligence Centre, or his or her representative
National Security Office

For the Republic of Peru:

Minister of Defence or his or her representative

2. Both authorities, each within the territory of its country, shall ensure the protection of the classified information transmitted in accordance with their national laws and regulations and the provisions of this Agreement.

3. In order to attain and maintain comparable levels of security, the competent authorities shall, upon request, provide each other with information on their security laws, regulations, organization and procedures and allow visits to their territory by duly accredited representatives of the other Party.

4. Upon request, the Parties, through their competent authorities, and taking into account their respective national laws, shall cooperate with each other during the procedures necessary for the granting of security clearance to their nationals who reside or who have resided in the territory of the other Party.

5. The competent authorities shall take appropriate measures to ensure that natural persons, organs or entities of their country having security clearance comply with the obligations of this Agreement.

Article 6. Security classification

1. The Parties agree that the following security classification levels are equivalent:	
Kingdom of Spain	Republic of Peru
RESERVADO (RESERVED)	SECRETO (SECRET)
CONFIDENCIAL (CONFIDENTIAL)	RESERVADO (RESERVED)
DIFUSIÓN LIMITADA (RESTRICTED)	CONFIDENCIAL (CONFIDENTIAL)

2. The Receiving Party shall classify the information received at a level equivalent to that assigned by the Originating Party, in accordance with the preceding paragraph.

3. The Receiving Party shall not be able to reclassify or declassify the received classified information without the prior written authorization of the competent authority of the Originating Party.

4. The Originating Party shall inform the Receiving Party of any reclassification or declassification of the classified information transmitted.

Article 7. Handling of classified information

1. No one shall be authorized to access classified information on the sole basis of rank or appointment or by virtue of holding a personal security clearance. Access to classified information shall be granted solely to those persons with a need to know who have obtained the relevant

clearance and the corresponding authorization to access the information, in accordance with the national laws and regulations of the relevant Party.

2. The Parties shall accept the personal security clearance issued by the competent authority of the other Party.

3. Upon request, the Parties, through their competent authorities, and taking into account their respective national laws and regulations, shall assist each other in the implementation of clearance procedures relating to personal security clearances and/or facility security clearances. The competent authorities of both Parties may agree on specific mechanisms for this purpose.

4. Classified information that is exchanged may be used solely for the purposes for which it was transmitted.

Article 8. Translation, reproduction and destruction of classified information

1. Translations and reproductions of classified information shall be produced in accordance with the following procedures:

- (a) Translations and reproductions of classified information may be produced solely by individuals who have the appropriate clearance, and who hold a personal security clearance at the security classification level of the classified information being reproduced or translated;
- (b) The number of copies made shall be restricted to the quantity required for official purposes;
- (c) Copies shall be marked with the same classification level as the original classified information and shall be controlled by the Parties; and
- (d) Classified information classified RESERVADO (RESERVED) by Spain and SECRETO (SECRET) by Peru may be reproduced only when the competent authority of the Receiving Party has received written authorization from the competent authority of the Originating Party.

2. Destruction of classified information shall be carried out in accordance with the national laws and regulations of the Receiving Party when the information is no longer deemed necessary, so as to prevent its total or partial reconstruction or identification.

3. Information classified as RESERVADO (RESERVED) by Spain and SECRETO (SECRET) by Peru may be destroyed only with the prior written consent of the Originating Party.

Article 9. Transmission of classified information

1. Classified information shall be transmitted between the Parties through the diplomatic channel, or through natural persons, organs or entities duly cleared and authorized by the Originating Party and in accordance with procedures mutually agreed by the competent authorities of the Parties.

2. Classified information may be transmitted solely through protected communications systems, networks or other electromagnetic media approved and authorized by the competent authorities of both Parties.

3. The transmission of large amounts of classified information shall be authorized, on a case-by-case basis, by both competent authorities.

4. The competent authority of the Receiving Party shall acknowledge, in writing, receipt of the classified information.

5. The Receiving Party shall not transmit classified information to any third party or to any natural person, organ or entity that holds the nationality of a third State without the prior written authorization of the Originating Party.

Article 10. Classified information carriers

1. Classified information carriers received shall be marked by the receiving entity at the equivalent level of classification, in accordance with article 6 of this Agreement.

2. The obligation to mark with the equivalent levels of classification established shall extend to classified information carriers generated in the process of joint cooperation between the Parties, as well as that generated as a result of translations or reproductions.

3. Classified information carriers shall be destroyed in accordance with the national law of the Receiving Party when they are no longer deemed necessary, with the prior authorization of the Originating Party. The destruction shall make the total or partial recovery or reproduction of the classified information impossible.

4. Other specifications regarding how to process classified information carriers shall be made in accordance with the national laws and regulations of the Parties.

Article 11. Classified contracts

1. Any Party that wishes to enter into a classified contract with a contractor of the other Party, or to authorize one of its own contractors to enter into a classified contract in the territory of the other Party, shall obtain prior written assurance from the competent authority of the other Party that the proposed contractor holds a facility security clearance at the appropriate level.

2. In accordance with the preceding paragraph, all subcontractors shall also be cleared and undertake to protect classified information, in accordance with paragraph 5 of this article.

3. Classified contracts shall be entered into and executed in accordance with the national laws and regulations of each Party.

4. Each classified contract or subcontract shall include, as an integral part thereof, a security annex on the protection of classified information, covering the following:

- (a) Identification of classified information;
- (b) Security instructions on the project establishing the set of procedures and security measures applicable to classified information;
- (c) Liabilities for damages arising from any security breach;
- (d) Obligation to report any security breach to the relevant competent authority;
- (e) Specification of communication channels or media for the transmission of classified information;
- (f) Obligation of the contractor, its employees, officers or representatives to maintain the appropriate level of confidentiality; and
- (g) Liabilities for non-compliance with the security procedures and measures applicable to classified information.

5. The contractor's responsibility to protect classified information shall include, at a minimum, the obligation to:

- (a) Grant access to classified information solely to persons who hold a personal security clearance and have a need to know;
- (b) Specify the means needed to transmit classified information securely;
- (c) Establish procedures for visits by staff from one Party to the other Party;
- (d) Inform its competent authority of any unauthorized access, attempted access or suspected access to the classified information exchanged;
- (e) Use the classified information received solely for the purposes for which it was transmitted; and
- (f) Comply with the procedures established by the respective laws and regulations regarding the handling of classified information, in accordance with the national laws of the Parties and the provisions of this Agreement.

6. A copy of each classified contract or subcontract shall be sent to the competent authority of the Party in whose territory the classified contract or subcontract is to be executed, in order to verify compliance with the security clauses.

7. Should any event occur that renders the retention of transmitted classified information unnecessary, all classified information exchanged or generated under a classified contract shall be destroyed, in accordance with the national laws and regulations of the Receiving Party.

Article 12. Visits

1. Visits by nationals of one Party to the other Party involving access to classified information shall be subject to prior written authorization by the competent authority of the host Party, and shall be conducted in accordance with the national laws and regulations of that Party.

2. Requests for visits shall be submitted through the competent authorities at least 20 days prior to the scheduled date of the visit.

3. Each Party shall authorize visits by the other Party only when the visitors:

- (a) Hold a valid personal security clearance granted by their country of origin; and
- (b) Are authorized to receive or have access to classified information owing to a need to know.

4. Requests for visits shall be submitted through the competent authority and shall include the following information:

- (a) Visitor's personal information: full name, place and date of birth, nationality, passport or other identity document number;
- (b) Name of the organ or entity to which the visitor belongs;
- (c) Information related to the visit: period of the visit, object and purpose of the visit, name of the entity or entities to be visited;
- (d) Names, surnames and telephone number and/or email address of a designated contact person in the body or entity to be visited;
- (e) Level of classification of the information to be accessed; and

(f) Certification of visitor security clearance displaying the level of classification, the period of validity and any restrictions stated therein.

5. The competent authority of the host country shall notify the competent authority of the visitor's country of its decision at least 10 days prior to the scheduled date of the visit.

6. Once the visit has been authorized, the competent authority of the host Party shall forward a copy of the visit request to the entity to be visited. The latter shall inform the visitor of the corresponding regulations and procedures to be observed during the visit.

7. All visitors shall comply with the security regulations and procedures in place for access to the facilities to be visited. Visitors shall not disclose to unauthorized third parties the classified information to which they had access during their visit.

8. In the case of classified contracts requiring periodic visits, the Parties may draw up lists of authorized persons. Such lists shall not be valid for more than 12 months.

9. Each Party shall protect the personal information of visitors in accordance with the applicable national laws and regulations.

Article 13. Security breach

1. In the event of a security breach involving classified information, the competent authority of the Party where the security breach occurred shall immediately inform the competent authority of the other Party.

2. The Party in which the security breach occurred shall investigate or cooperate in the investigation of the incident and inform the other Party as soon as possible of the outcome of the investigation and the applicable remedial actions.

Article 14.. Expenses

1. This Agreement does not provide for any expenses to be incurred.

2. If any expenses are incurred, each Party shall bear its own expenses arising from the implementation and monitoring of all aspects of this Agreement, in accordance with its national laws and regulations.

Article 15. Settlement of disputes

1. Any dispute regarding the interpretation or implementation of this Agreement shall be settled by consultation between the Parties through the diplomatic channel.

2. While the dispute is being settled, the Parties shall continue to comply with their obligations under this Agreement, in accordance with the preceding paragraph.

Article 16. Final provisions

1. This Agreement shall enter into force 30 days after the date of receipt of the last notification in which the Parties inform each other, through the diplomatic channel, that the legal procedures required under their respective legal systems have been completed; it shall remain in force indefinitely.

2. This Agreement may be amended with the written mutual consent of both Parties. Any amendments shall enter into force in accordance with the preceding paragraph.

3. Either Party may terminate this Agreement by giving notice in writing to the other Party through the diplomatic channel. The termination shall take effect six months following receipt of the notification by the other Party.

4. Notwithstanding the termination, all classified information transmitted pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein until the Originating Party declassifies the information or decides on or authorizes its destruction.

DONE at Madrid on 28 February 2019, in two copies, both texts being equally authentic.

For the Kingdom of Spain:
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN
President of Spain

For the Republic of Peru:
MARTÍN VIZCARRA CORNEJO
President of Peru

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LA RÉPUBLIQUE DU PÉROU
RELATIF À L'ÉCHANGE ET LA PROTECTION RÉCIPROQUE DES
INFORMATIONS CLASSIFIÉES DANS LE DOMAINE DE LA DÉFENSE

Le Royaume d'Espagne et la République du Pérou,
ci-après dénommés les « Parties »,

Désireux d'assurer la protection des informations classifiées échangées ou produites dans le domaine de la défense,

Tenant compte de leur intérêt mutuel à assurer la protection des informations classifiées dans ce domaine, conformément aux lois et réglementations nationales des Parties,

Sont convenues de ce qui suit :

ARTICLE PREMIER. CHAMP D'APPLICATION

Le présent Accord établit les règles et procédures de protection des informations classifiées dans le domaine de la défense, qui sont échangées entre les Parties ou produites par celles-ci, les personnes physiques, les organismes ou les entités accréditées relevant de leur juridiction.

ARTICLE 2. OBLIGATIONS GÉNÉRALES

1. Les deux Parties prennent toutes les mesures nécessaires pour assurer la protection des informations classifiées transmises ou produites dans le cadre du présent Accord, conformément à leurs lois et réglementations nationales.

2. Aucune des Parties ne peut invoquer le présent Accord en vue d'obtenir des informations classifiées que l'autre Partie a reçues d'une tierce partie.

ARTICLE 3. DROITS DE PROPRIÉTÉ INTELLECTUELLE

1. La protection de la propriété intellectuelle est régie par les législations nationales respectives des Parties et les accords internationaux en la matière qui s'appliquent aux deux Parties.

2. Aucune disposition du présent Accord ne réduit ni ne limite les droits de propriété intellectuelle associés aux informations classifiées échangées que détiennent l'une ou l'autre des Parties, ses contractants ou des tiers.

3. Les droits de propriété intellectuelle relatifs aux informations classifiées produites dans le cadre du présent Accord sont définis par les Parties conformément à leurs lois et réglementations nationales respectives.

ARTICLE 4. DÉFINITIONS

Aux fins du présent Accord :

- a) le terme « informations classifiées » désigne toute information, quel que soit sa forme, sa nature ou son mode de transmission, nécessitant une protection contre toute divulgation non autorisée ou toute perte, et à laquelle une classification de sécurité a été attribuée conformément aux lois et réglementations nationales des Parties ;
- b) le terme « supports d'informations classifiées » désigne les objets physiques sur lesquels les informations classifiées sont enregistrées sous forme de symboles, d'images, de signes, de règles techniques et de processus. Leur protection est régie par la législation nationale de chaque Partie ;
- c) le terme « autorité compétente » désigne l'autorité désignée par chaque Partie et chargée de la mise en œuvre et la supervision du présent Accord, telle que désignée à l'article 5 ;
- d) le terme « Partie d'origine » désigne la Partie qui fournit les informations classifiées ;
- e) le terme « Partie destinataire » désigne la Partie à laquelle la Partie d'origine transmet des informations classifiées ;
- f) le terme « tierce partie » désigne toute organisation internationale ou tout État qui n'est pas l'une des Parties au présent Accord ;
- g) le terme « consignes de sécurité » désigne l'ensemble des procédures et des mesures de sécurité supplémentaires visant à protéger les informations classifiées définies dans un contrat classifié particulier ;
- h) le terme « contrat classifié » désigne tout contrat, toute convention ou tout accord de coopération dont l'objet ou l'application implique l'accès à des informations classifiées ou leur gestion, à savoir la production, le traitement ou le stockage desdites informations, dans le cadre du présent Accord ;
- i) le terme « contrat de sous-traitance classifié » désigne tout contrat, toute convention ou tout accord de coopération dont l'objet ou l'application implique l'accès à des informations classifiées ou leur gestion, à savoir la production, le traitement ou le stockage desdites informations, dans le cadre du présent Accord ;
- j) les termes « contractant » ou « sous-traitant » désignent l'entité juridique ou la personne physique, accréditée par l'autorité compétente, ayant la capacité de conclure un contrat classifié conformément au présent Accord, ainsi qu'aux lois et réglementations nationales des Parties ;
- k) le terme « compromission de la sécurité » désigne tout acte ou omission, intentionnel ou accidentel, entraînant la compromission ou le risque de compromission des informations classifiées ;
- l) le terme « habilitation de sécurité individuelle » désigne la décision prise par l'autorité compétente, attestant qu'une personne satisfait aux exigences pour accéder aux informations classifiées, conformément aux lois et réglementations respectives des Parties ;
- m) le terme « habilitation de sécurité d'établissement » désigne la décision prise par l'autorité compétente, attestant qu'un établissement possède, du point de vue de la sécurité, la capacité physique et organisationnelle pour produire, stocker et gérer des

informations classifiées, conformément aux lois et réglementations respectives des Parties ;

- n) le terme « besoin d'en connaître » désigne le principe selon lequel une personne peut uniquement accéder aux informations classifiées s'il est démontré qu'elle en a besoin pour s'acquitter de ses fonctions officielles, dans le cadre desquelles lesdites informations sont divulguées à la Partie destinataire.

ARTICLE 5. AUTORITÉS COMPÉTENTES

1. Les autorités compétentes responsables de l'application du présent Accord sont les suivantes :

Pour le Royaume d'Espagne :

le Secrétaire d'État, le directeur du Centre national du renseignement ou son représentant,
le Bureau de la sécurité nationale ;

Pour la République du Pérou :

le Ministre de la défense ou son représentant.

2. Les deux autorités assurent, sur le territoire de leur pays respectif, la protection des informations classifiées transmises conformément à leurs lois et règlements nationaux et aux dispositions du présent Accord.

3. En vue d'atteindre et de maintenir des niveaux de sécurité similaires, les autorités compétentes se tiennent mutuellement informées, sur demande, de leur législation, leur réglementation, leur organisation et leurs procédures en matière de sécurité et autorisent les visites, sur leur territoire, des représentants dûment accrédités de l'autre Partie.

4. Sur demande et conformément à leur législation nationale respective, les Parties collaborent entre elles, par l'intermédiaire de leurs autorités compétentes, au cours des procédures nécessaires à l'habilitation de sécurité de leurs ressortissants résidant ou ayant résidé sur le territoire de l'autre Partie.

5. Les autorités compétentes prennent les mesures appropriées pour s'assurer que les personnes physiques, les organismes ou les entités accréditées de leur pays se conforment aux obligations du présent Accord.

ARTICLE 6. CLASSIFICATION DE SÉCURITÉ

Royaume d'Espagne	Équivalent en français	République du Pérou	Équivalent en français
RESERVADO	RESTREINT	SECRETO	SECRET
CONFIDENCIAL	CONFIDENTIEL	RESERVADO	RESTREINT
DIFUSIÓN LIMITADA	DIFFUSION LIMITÉE	CONFIDENCIAL	CONFIDENTIEL

1. Les Parties conviennent que les niveaux de classification suivants sont équivalents :

2. La Partie destinataire accorde aux informations classifiées reçues un niveau de classification équivalent à celui attribué par la Partie d'origine, conformément aux dispositions du paragraphe précédent.

3. La Partie destinataire ne peut reclassifier ou déclassifier les informations classifiées reçues sans l'autorisation écrite préalable de l'autorité compétente de la Partie d'origine.

4. La Partie d'origine informe la Partie destinataire de toute reclassification ou déclassification des informations classifiées transmises.

ARTICLE 7. GESTION DES INFORMATIONS CLASSIFIÉES

1. Nul n'est autorisé à accéder aux informations classifiées au seul motif de son rang ou de sa nomination, ou du fait qu'il détient une habilitation de sécurité individuelle. Conformément aux lois et réglementations nationales de la Partie concernée, l'accès aux informations classifiées n'est accordé qu'aux personnes ayant besoin d'en connaître qui ont obtenu l'habilitation appropriée et l'autorisation d'accès correspondante.

2. Les Parties acceptent l'habilitation de sécurité individuelle délivrée par l'autorité compétente de l'autre Partie.

3. Sur demande et conformément à leurs lois et réglementations nationales respectives, les Parties, par l'intermédiaire de leurs autorités compétentes, se prêtent mutuellement assistance dans le cadre de la mise en œuvre des procédures d'habilitation relatives aux habilitations de sécurité individuelle et aux habilitations de sécurité d'établissement. Les autorités compétentes des deux Parties conviennent des mécanismes spécifiques à mettre en place à cet effet.

4. Les informations classifiées échangées ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été transmises.

ARTICLE 8. TRADUCTION, REPRODUCTION ET DESTRUCTION D'INFORMATIONS CLASSIFIÉES

1. Les traductions et les reproductions d'informations classifiées se font conformément aux procédures suivantes :

- a) seules les personnes disposant de l'autorisation correspondante et titulaires d'une habilitation de sécurité individuelle du niveau de classification de sécurité des informations classifiées reproduites ou traduites peuvent procéder à la traduction et la reproduction d'informations classifiées ;
- b) le nombre de copies se limite à celui requis pour un usage officiel ;
- c) les copies portent la même classification que les informations classifiées originales et sont contrôlées par les Parties ;
- d) la reproduction des informations classifiées *RESERVADO* pour la Partie espagnole et *SECRETO* pour la Partie péruvienne est uniquement autorisée si l'autorité compétente de la Partie destinataire a reçu l'accord écrit de l'autorité compétente de la Partie d'origine.

2. Les informations classifiées sont détruites conformément aux lois et réglementations nationales de la Partie destinataire lorsqu'elles ne sont plus jugées nécessaires, de manière à empêcher leur reconstitution ou leur reconnaissance intégrale ou partielle.

3. Les informations classifiées RESERVADO pour la Partie espagnole et SECRETO pour la Partie péruvienne peuvent uniquement être détruites avec l'accord écrit préalable de la Partie d'origine.

ARTICLE 9. TRANSMISSION D'INFORMATIONS CLASSIFIÉES

1. Les Parties se transmettent les informations classifiées par la voie diplomatique ou par l'intermédiaire de personnes physiques, d'organismes ou d'entités dûment habilités et autorisés par la Partie d'origine, conformément aux procédures convenues d'un commun accord entre les autorités compétentes des Parties.

2. La transmission des informations classifiées ne s'effectue que par des systèmes de communication sécurisés, des réseaux ou d'autres moyens électromagnétiques approuvés et autorisés par les autorités compétentes des deux Parties.

3. Les deux autorités compétentes approuvent, au cas par cas, la transmission d'informations classifiées volumineuses ou en grandes quantités.

4. L'autorité compétente de la Partie destinataire confirme par écrit la réception des informations classifiées.

5. La Partie destinataire ne transmet aucune information classifiée à une quelconque tierce partie ou à une personne physique, un organisme ou une entité d'un État tiers sans l'autorisation écrite préalable de la Partie d'origine.

ARTICLE 10. SUPPORTS D'INFORMATIONS CLASSIFIÉES

1. L'entité destinataire indique sur les supports d'information classifiés reçus le niveau de classification équivalent conformément à l'article 6 du présent Accord.

2. L'obligation de préciser les niveaux de classification équivalents établis des informations classifiées s'étend aux supports d'informations classifiées produites dans le cadre du processus de coopération conjointe des Parties, ainsi qu'aux informations générées à la suite de traductions ou de reproductions.

3. La destruction des supports d'information classifiés s'effectue conformément à la législation nationale de la Partie destinataire, et avec l'autorisation de la Partie d'origine, lorsqu'ils ne sont plus jugés nécessaires. La destruction doit rendre impossible la récupération ou la reproduction intégrale ou partielle des informations classifiées.

4. Les autres spécifications relatives au traitement des supports d'informations classifiées sont établies conformément aux lois et réglementations nationales des Parties.

ARTICLE 11. CONTRATS CLASSIFIÉS

1. Si une Partie souhaite conclure un contrat classifié avec un contractant de l'autre Partie, ou si l'un de ses contractants conclut un contrat classifié sur le territoire de l'autre Partie, elle doit obtenir au préalable l'assurance écrite de l'autorité compétente de l'autre Partie précisant que le

contractant est bien titulaire d'une habilitation de sécurité d'établissement du niveau de classification approprié.

2. Conformément au paragraphe précédent, tout sous-traitant doit également disposer d'une habilitation et s'engager à protéger les informations classifiées conformément au paragraphe 5 du présent article.

3. Les contrats classifiés sont conclus et exécutés conformément aux lois et réglementations nationales de chaque Partie.

4. Chaque contrat classifié ou contrat de sous-traitance classifié comprend une annexe relative à la protection des informations classifiées, laquelle en fait partie intégrante et couvre les aspects suivants :

- a) l'identification des informations classifiées ;
- b) les consignes de sécurité du projet définissant l'ensemble des procédures et des mesures de sécurité applicables aux informations classifiées ;
- c) la responsabilité en matière de dommages résultant d'une compromission quelconque de la sécurité ;
- d) l'obligation de signaler toute compromission de la sécurité à l'autorité compétente concernée ;
- e) la mise à disposition de canaux de communication ou de moyens pour la transmission d'informations classifiées ;
- f) l'obligation pour le contractant, ses employés, ses dirigeants ou ses représentants de garantir le niveau de confidentialité adéquat ;
- g) la responsabilité en matière d'inexécution des procédures et des mesures de sécurité applicables aux informations classifiées.

5. La responsabilité du contractant en matière de protection des informations classifiées s'étend, au minimum, à l'obligation :

- a) de donner uniquement accès aux informations classifiées aux personnes titulaires d'une habilitation de sécurité individuelle et ayant besoin d'en connaître ;
- b) de mettre en place les moyens nécessaires pour transmettre en toute sécurité des informations classifiées ;
- c) d'établir des procédures pour les visites du personnel d'une Partie à l'autre ;
- d) de signaler tout accès, toute tentative d'accès ou toute suspicion d'accès non autorisé aux informations classifiées échangées à son autorité compétente ;
- e) d'utiliser uniquement les informations classifiées aux fins pour lesquelles elles ont été transmises ;
- f) de se conformer aux procédures établies par les lois et réglementations respectives concernant la gestion des informations classifiées, conformément aux lois nationales des Parties et aux dispositions du présent Accord.

6. Une copie de chaque contrat ou contrat de sous-traitance classifié est transmise à l'autorité compétente de la Partie sur le territoire de laquelle le contrat classifié ou le contrat de sous-traitance classifié est exécuté, afin de vérifier le respect des clauses de sécurité.

7. En cas d'événement rendant inutile la conservation des informations classifiées transmises, toutes les informations classifiées échangées ou produites dans le cadre d'un contrat

classifié sont détruites, conformément aux lois et réglementations nationales de la Partie destinataire.

ARTICLE 12. VISITES

1. Les visites de ressortissants d'une Partie dans l'autre Partie, impliquant l'accès à des informations classifiées, sont soumises à l'autorisation préalable, par écrit, de l'autorité compétente de la Partie hôte, et se déroulent conformément aux lois et réglementations nationales de cette Partie.

2. La demande de visite est présentée par l'intermédiaire des autorités compétentes au moins vingt jours avant la date prévue de la visite.

3. Chaque Partie autorise les visites de l'autre Partie uniquement lorsque les visiteurs :

- a) sont titulaires d'une habilitation de sécurité individuelle valide délivrée par leur pays d'origine ;
- b) sont autorisés à recevoir des informations classifiées ou à y avoir accès en application du principe du besoin d'en connaître.

4. La demande de visite est présentée par l'intermédiaire de l'autorité compétente et doit inclure les informations suivantes :

- a) les données personnelles du visiteur (nom et prénom, date et lieu de naissance, nationalité, numéro de passeport ou d'un autre document d'identité) ;
- b) l'organisme ou l'entité à laquelle appartient le visiteur ;
- c) les données relatives à la visite (date, objet et but de la visite, l'entité ou les entités à visiter) ;
- d) les coordonnées d'un point de contact au sein de l'organisme ou de l'entité à visiter (nom et prénom, numéro de téléphone et/ou adresse électronique) ;
- e) le niveau de classification des informations auxquelles les visiteurs souhaitent accéder ;
- f) l'attestation de détention d'une habilitation de sécurité pour le visiteur, sur laquelle figurent le niveau de classification, la durée de validité et les éventuelles restrictions mentionnées sur l'habilitation de sécurité du visiteur.

5. L'autorité compétente du pays hôte informe l'autorité compétente du pays du visiteur de sa décision au moins dix jours avant la date prévue de la visite.

6. Une fois la visite autorisée, l'autorité compétente de la Partie hôte transmet une copie de la demande de visite à l'entité qui sera visitée. Celle-ci informe le visiteur des règles et procédures appropriées qu'il devra suivre pendant la visite.

7. Tous les visiteurs doivent se conformer aux règles de sécurité et aux procédures d'accès aux installations à visiter. Les visiteurs ne doivent pas divulguer à des tiers non autorisés les informations classifiées auxquelles ils ont accès au cours de leur visite.

8. Pour ce qui est des contrats classifiés nécessitant des visites périodiques, les Parties peuvent établir des listes de personnes autorisées. La durée de validité de ces listes ne peut excéder douze mois.

9. Chaque Partie protège les données à caractère personnel des visiteurs conformément aux lois et réglementations nationales applicables.

ARTICLE 13. COMPROMISSION DE LA SÉCURITÉ

1. En cas de compromission de la sécurité d'informations classifiées, l'autorité compétente de la Partie où est survenue cette compromission de la sécurité en informe immédiatement l'autorité compétente de l'autre Partie.

2. La Partie où est survenue la compromission de la sécurité ouvre une enquête ou collabore à l'enquête relative à l'incident et informe l'autre Partie dès que possible des résultats de l'enquête et des mesures correctives applicables.

ARTICLE 14. FRAIS

1. Le présent Accord ne prévoit aucune dépense spécifique.

2. Si des frais sont occasionnés du fait de l'exécution et de la supervision de tous les aspects du présent Accord, chaque Partie les supporte conformément à ses lois et réglementations nationales.

ARTICLE 15. RÈGLEMENT DES DIFFÉRENDS

1. Tout différend concernant l'interprétation ou l'application du présent Accord est résolu au moyen de négociations, par la voie diplomatique, entre les Parties.

2. Lors de la période de règlement des différends visée au paragraphe précédent, les Parties continuent à respecter les obligations qui leur incombent en vertu du présent Accord.

ARTICLE 16. DISPOSITIONS FINALES

1. Le présent Accord est conclu pour une durée indéterminée et entre en vigueur trente jours après la date de réception de la dernière des notifications écrites échangées par les Parties et par lesquelles elles se sont tenues informées, par la voie diplomatique, de l'accomplissement des procédures requises par leurs systèmes juridiques respectifs à cet effet.

2. Le présent Accord peut être modifié d'un commun accord, par écrit, entre les Parties. Les modifications entrent en vigueur conformément aux dispositions du paragraphe précédent.

3. Chacune des Parties peut dénoncer le présent Accord moyennant une notification écrite transmise par la voie diplomatique à l'autre Partie. La dénonciation prend effet six mois après la date de réception de la notification par l'autre Partie.

4. Nonobstant la dénonciation du présent Accord, toutes les informations classifiées transmises en vertu de celui-ci continuent d'être protégées conformément à ses dispositions jusqu'à ce que la Partie d'origine déclassifie les informations ou décide de la destruction desdites informations.

FAIT à Madrid le 28 février 2019 en deux exemplaires, les deux textes faisant également foi.

Pour le Royaume d'Espagne :
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN
Premier ministre de l'Espagne

Pour la République du Pérou :
MARTÍN VIZCARRA CORNEJO
Président de la République du Pérou