No. 56618*

Spain
and
New Zealand

Agreement between the Kingdom of Spain and the Government of New Zealand relating to the protection of classified information (with annex). Madrid, 16 December 2019

Entry into force: *17 March 2021 by notification, in accordance with article 19(1)*

Authentic texts: *English and Spanish*

Registration with the Secretariat of the United Nations: *Spain, 31 March 2021*

*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
Nouvelle-Zélande

Accord entre le Royaume d'Espagne et le Gouvernement de la Nouvelle-Zélande relatif à la protection d'informations classifiées (avec annexe). Madrid, 16 décembre 2019

Entrée en vigueur : *17 mars 2021 par notification, conformément au paragraphe 1 de l'article 19*

Textes authentiques : *anglais et espagnol*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Espagne, 31 mars 2021*

*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.

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT

BETWEEN

THE KINGDOM OF SPAIN

AND

THE GOVERNMENT OF NEW ZEALAND

RELATING TO

THE PROTECTION OF CLASSIFIED INFORMATION

The Kingdom of Spain

and

The Government of New Zealand

hereinafter referred to as "the Parties"

Having an interest in the protection of defence classified information

Desiring to establish the conditions for the protection of defence classified information and materials exchanged or developed, by the Parties including provisions for exchange with public or private bodies in accordance with the Parties' respective national laws and regulations,

have agreed as follows:

ARTICLE 1
DEFINITIONS

For the purposes of this Agreement,

"**Classified contract**", means a contract, sub-contract or a project where access to classified information is required or where classified information may be generated;

"**Classified information**" means information that is generated by or for the Kingdom of Spain or the Government of New Zealand, or that is under the jurisdiction or control of one of them, and which requires protection in the interests of national security and that is so designated by the assignment of a security classification in accordance with the national laws and regulations of the Party or Parties. The information may be in oral, visual, electronic, or documentary form, or in the form of material including, equipment or technology.

"**Competent Security Authority**" or "**CSA**" means the authority designated under the law of the Government of the State with ultimate responsibility for the implementation of the provisions of this Agreement and the transmission of classified information to the other Party;

"**Contractor**" means any person or body with the legal capacity to enter into contracts.

"**Facility Security Clearance**" or "**FSC**" means a determination by a CSA of a Party that a Contractor has in place appropriate security measures within a specified facility to protect classified information up to and including a particular Security Classification Level.

"**Host Party**" means the Party in whose territory a visit takes place;

"**Need to know**" refers to the need for access to classified information as part of a recognised official function for a specific authorised purpose;

"**Originating Party**" means the Party that creates, delivers or transmits classified information to the Receiving Party;

"**Originating User**" means a public or private individual, agency or organisation that is contracted or authorised by the Originating Party to create, deliver, or transmit classified information for the Originating Party;

"**Personnel Security Clearance**" or "**PSC**" means a determination by a CSA that an individual has been security cleared to access and handle classified information up to and including a specified Security Classification Level in accordance with its national laws and regulations.

"**Receiving Party**" means the Party that is the recipient of classified information that is transmitted by the Originating Party.

"**Receiving User**" means a public or private individual, agency or organisation that is contracted or authorised by the Receiving Party to handle classified information for the Receiving Party;

"**Security Classification Level**" means a category assigned to classified information which indicates its sensitivity, the degree of damage that might arise in the event of its unauthorised disclosure or loss and the level of protection to be applied to it by the Parties.

"**Security Incident**" means an act or omission contrary to national laws and regulations which may or does result in the unauthorised access, disclosure, loss, destruction or compromise of classified information that has been generated and/or exchanged under this Agreement.

"**Third Party**" means any State, including legal entities and individuals under its jurisdiction, or International Organisation, which is not a Party to this Agreement.

ARTICLE 2
SCOPE

This Agreement regulates the exchange of all classified information pertaining to matters of defence between the Parties, or between public or private bodies subject to their national laws and regulations.

ARTICLE 3
COMPETENT SECURITY AUTHORITIES

1. The Competent Security Authorities responsible for the general control and putting in place of this Agreement are:

   a. **For the Kingdom of Spain:**
   Secretary of State Director of the National Intelligence Centre
   National Office of Security

   b. **For New Zealand:**
   Director General
   New Zealand Security Intelligence Service

2. The Parties shall keep each other informed in writing of all changes in the appointment of their CSAs. Any change to the CSA shall not constitute a formal amendment to this Agreement.

ARTICLE 4
PRINCIPLES OF SECURITY

1. In accordance with their national laws and regulations, the Parties shall take appropriate measures to protect classified information that is transmitted, received or generated under the terms of this Agreement and provide a level of protection equivalent to such information that is accorded to their own national classified information, as defined in Article 5.

2. The protection of classified information exchanged between the Parties is governed by the following principles:

   a) The Receiving Party shall give classified information that it receives a level of protection equivalent to that expressly applied to the information by the Originating Party, conforming to the equivalence defined in Article 5 of this Agreement.

b) Access to classified information is limited only to persons who have been given prior approval to the required level and whose duties require access to such classified information on a Need to know basis.

c) The Receiving Party shall not transmit classified information to a Third Party, without prior written approval of the CSA of the Originating Party.

d) Classified information may not be used for purposes other than those for which it is officially transmitted.

e) When an Originating Party changes the classification of any classified information exchanged pursuant to this Agreement, it shall advise the other Party in writing of that change.

f) The Receiving Party must not downgrade or declassify transmitted classified information without the prior written approval of the CSA of the Originating Party.

3. Conforming to the procedures stated in this Agreement, the CSAs or their approved representatives of each Party may upon request, visit the sites and installations on the territory of the other Party to examine the protection measures put in place to ensure the security of classified information which is transmitted pursuant to this Agreement.

ARTICLE 5
EQUIVALENT SECURITY CLASSIFICATIONS

1. The Parties, having taken account of the security measures prescribed by their respective national laws and regulations, commit to assuring the protection of exchanged classified information and adopt the equivalent level of security classifications as defined in the table below:

SPAIN	NEW ZEALAND
SECRETO	TOP SECRET
RESERVADO	SECRET
CONFIDENCIAL	CONFIDENTIAL
DIFUSIÓN LIMITADA	RESTRICTED

2. The Parties' security classifications are applied as follows:

For Spanish Classified Information

SECRETO, unauthorised disclosure or wrongful use would endanger or cause extreme damage to national interests;
RESERVADO, unauthorised disclosure or wrongful use would endanger or cause serious damage to national interests;
CONFIDENCIAL, unauthorised disclosure or wrongful use would endanger or cause damage to national interests;
DIFUSIÓN LIMITADA, unauthorised disclosure or wrongful use would be contrary to national interests.

For New Zealand Classified Information

TOP SECRET, compromise of information would damage national interests in an exceptionally grave manner;
SECRET, compromise of information would damage national interests in a serious manner;
CONFIDENTIAL, compromise of information would damage national interests in a significant manner;
RESTRICTED, compromise of information would damage national interests in an adverse manner.

3. The Parties shall keep each other informed in writing of any change concerning their respective national laws and regulations concerning the protection of classified information.

ARTICLE 6
PERSONNEL SECURITY CLEARANCES

1. No individual shall be entitled to access classified information solely by virtue of their rank, position or a PSC.

2. For access to information classified CONFIDENCIAL CONFIDENTIAL or higher, each Party shall, in accordance with national laws and regulations, ensure that each person who has access to, or may require access to classified information pursuant to this Agreement, is vetted to the same or higher security classification as the information accessed.

3. The CSAs of each Party shall, when necessary, assist in the provision of, or provide suitable notification of, the PSC of a national of a Party

residing in the territory of the other Party and requiring access to classified information.

4. A PSC is not required for access to classified information marked DIFUSIÓN LIMITADA / RESTRICTED. Such access shall be limited to individuals who have a Need to know, and who have been briefed on their responsibilities and obligations to protect such classified information.

ARTICLE 7
DISCLOSURE

1. Classified information exchanged, transmitted or generated jointly by the two Parties under this Agreement, including contracts or any other cooperative activities, may not be downgraded, declassified or transmitted to a Third Party, without prior written approval from the Originating Party.

2. Within the scope of national laws and regulations, the Receiving Party shall take all reasonable steps available to it to keep classified information free from disclosure. If there is any request to disclose any classified information provided under this Agreement, the Receiving Party shall immediately notify the Originating Party in writing, and both Parties shall consult each other in writing before a disclosure decision is taken by the Receiving Party.

ARTICLE 8
SECURITY COOPERATION

1. When the CSA of a Party requires confirmation of the FSC of a Contractor in the other Party, or the PSC of an individual in the other Party, it shall submit a formal written request to the CSA of that Party.

2. On receipt of such a request, the CSA shall notify the requesting CSA of the FSC or PSC status of the relevant Contractor or individual and the validity of the FSC or date of expiry of the PSC.

3. The CSAs shall assist each other in carrying out FSC and PSC security investigations on request and in accordance with national laws and regulations.

4. If, in accordance with national laws and regulations, a CSA withdraws or downgrades an existing FSC or PSC issued to a Contractor or

individual for which or for whom a confirmation has been provided, the CSA of the other Party shall be notified in writing as soon as is practicable.

ARTICLE 9
REPRODUCTION, TRANSLATION AND DESTRUCTION

1. Upon receipt of reproductions or translations of originals, the Receiving Party is to mark them as reproductions or translations accordingly. Such documents are to be afforded the same protection as the original document.

2. Translations shall contain a suitable annotation, in the language into which they have been translated, indicating that they contain classified information of the other Party.

3. Translations and reproductions shall be limited to the minimum required for an official purpose, and shall be made only by individuals with a Need to know and who hold a PSC to the Security Classification Level of the classified information being reproduced or translated.

4. Classified Information at the level of SECRETO / TOP SECRET shall only be translated or reproduced with the prior written permission of the CSA of the Originating Party.

5. Classified information shall be destroyed in accordance with the destruction standards prescribed in the respective Parties' national laws and regulations.

6. Upon destruction of a classified document or information by the Receiving Party, a written certificate of destruction must be held and provided to the Originating Party by the Receiving Party.

7. Classified Information at the level of SECRETO / TOP SECRET shall not be destroyed. It shall be returned to the Originating Party.

8. If a crisis situation makes it impossible to protect classified information provided under this Agreement, it shall be destroyed as soon as is practicable by using any appropriate means to avoid a Security Incident. The receiving Party shall notify the CSA of the Originating Party in writing should information classified RESERVADO / SECRET or

above provided under this Agreement need to be destroyed in a crisis situation.

ARTICLE 10
TRANSMISSION OF INFORMATION TO USERS

1. This Article applies to cases of transmission of classified information from:

   a) the Originating Party to the Receiving User via the Receiving Party;

   b) where the Originating Party and the Receiving Party have mutually agreed, the Originating Party directly to the Receiving User; and

   c) where the Originating Party and the Receiving Party have mutually agreed, the Originating User directly to the Receiving User.

2. Prior to the receipt of classified information (regardless of the recipient being the Receiving Party or the Receiving User), the CSA of the Receiving Party is to:

   a) ensure that its installations are in possession of the appropriate FSC;

   b) ensure that the individuals who will have access to classified information are in possession of the appropriate PSC;

   c) ensure that all persons who have access to classified information are informed of their responsibilities arising from national laws and regulations; and

   d) ensure the receipt of classified information is confirmed in writing to the Originating Party as soon as possible.

ARTICLE 11
TRANSMISSION BETWEEN PARTIES

1. Classified information is to be transmitted normally from one Party to the other through diplomatic channels or through other channels mutually agreed by the Parties in accordance with national laws and regulations of the Originating Party.

2. Transmissions are to meet the following requirements:

   a) The Originating Party is to ensure that the individual transmitting the information:

      i. is a government employee or is an employee of the Originating Party or Originating User, and
      ii. is in possession of a PSC to at least the level of the classified information being transmitted.

   b) The person that delivers the classified information is to carry a letter from the CSA that outlines;
      i. the authority for the individual to carry classified information;
      ii. the point of contact for the Originating Party; and
      iii. the point of contact for the Receiving Party.

   c) The Originating Party shall take a record of classified information that is transferred and provide a copy of this record to the Receiving Party upon request. Both Parties will convey the details of the record to their CSAs.

   d) Classified information shall be properly packaged and sealed in accordance with the national laws and regulations of the Originating Party;

3. Electronic transmission of classified information is to be made in encrypted form only, using encryption methods and devices mutually determined by the respective CSAs.

ARTICLE 12
CLASSIFIED CONTRACTS

1. If the CSA of one Party proposes to place, or a Contractor under its jurisdiction proposes to place, a classified contract involving classified information marked CONFIDENCIAL / CONFIDENTIAL or above with a Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the CSA of the other Party, in accordance with Article 8 of this Agreement, that the Contractor has been granted an FSC and/or PSC to the appropriate Security Classification Level.

2. The CSA which has granted a FSC or PSC shall be responsible for ensuring that the security conduct of that Contractor is in accordance with its national laws and regulations.

3. A FSC and/or PSC is not required for classified contracts that are limited to classified information at the DIFUSIÓN LIMITADA / RESTRICTED level.

4. Any contract or subcontract involving classified information shall include provisions concerning protection of such information. These provisions shall give effect to the provisions of this Agreement and to any other conditions on the use of classified information imposed by the Originating Party. Only the Originating Party may modify the level of classification of information or authorise further disclosure.

5. The CSA of the Originating Party shall transmit a copy of the security provisions in a contract to the CSA of the Receiving Party.

ARTICLE 13
VISITS

1. Visits by nationals of a Party onto the site of the other Party where classified information is held, are permitted provided that prior written approval for such visits has been given by the CSA of the Host Party. Visits by nationals of third States to areas where classified information is exchanged between the Parties may only be authorised upon the mutual agreement of the Parties.

2. Requests for visits by a Party shall be transmitted through diplomatic channels to the CSA of the Host Party at least three weeks before the

date of the visit. The requests for visits shall contain the information specified in Annex A to this Agreement.

3. A Party may request permission to visit for a maximum period of twelve months. If a particular visit may not be concluded within the period specified by the authorisation to visit, or if an extension of the period covered by the authorisation of access is required, the Requesting Party may request a new authorisation visit provided it is carried out at least three weeks before the current authorisation expires.

4. All visitors must comply with the national laws and regulations of the Host Party concerning the protection of classified information.

5. Visits will be authorised only if the individual is in possession of the appropriate PSC and has a Need to know.

ARTICLE 14
MULTIPLE VISITS

1. For any project, programme or classified contract, the Parties may draw up lists of authorised personnel to make multiple visits in accordance with the terms and conditions agreed upon by the CSAs of the Parties. Initially, these lists are valid for a period of twelve months, and, by agreement between the CSAs of the Parties, the validity period may be extended for further periods not exceeding twelve months in total.

2. Once such a list has been approved by the host CSA, visit arrangements may be agreed directly between the facilities involved.

ARTICLE 15
SECURITY INCIDENTS

1. In the event of a suspected or confirmed Security Incident concerning classified information of the other Party, this shall be investigated by the Party where the incident occurs and the CSA of the other Party shall be immediately informed in writing.

2. Notification must be sufficiently detailed so that the Originating Party can start a complete evaluation of the consequences.

3. The Receiving Party shall lead an inquiry (with, if necessary, the help of the other Party) and take all appropriate measures, in accordance with its

national laws and regulations, in order to limit the consequences. The Receiving Party shall inform the Originating Party of the results of the enquiry and of all measures taken to avoid a recurrence.

ARTICLE 16
COSTS

In the case of any cost, each Party shall bear its own costs in relation to activities conducted pursuant to this Agreement.

ARTICLE 17
RESOLUTION OF DISPUTES

Any dispute relating to the interpretation or the application of this Agreement shall be settled exclusively by consultation between the Parties.

ARTICLE 18
INTELLECTUAL PROPERTY RIGHTS

Nothing in this Agreement diminishes or limits any intellectual property (including patents and copyright) associated with transferred classified information to which either Party, it's Contractors or any Third Party may be entitled.

ARTICLE 19
FINAL PROVISIONS

1. Each Party shall notify the other Party in writing of the completion of its internal procedures necessary to bring this Agreement into force, which shall occur on the day the second notification is received.

2. This Agreement may be amended at any time by the mutual, written consent of the Parties. Amendments will enter into force by the same procedure as described in Paragraph 1 of this Article.

3. The Annex forms an integral part of this Agreement.

4. The CSAs may conclude Implementing Arrangements pursuant to this Agreement.

5. This Agreement shall remain in force for an indefinite period. Either Party may terminate the Agreement by giving six months notice in writing through diplomatic channels to the other Party.

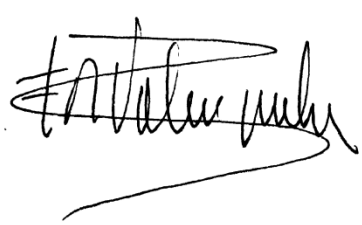
6. Obligations concerning the protection of classified information exchanged under this Agreement shall continue notwithstanding termination of the Agreement.

7. In the event of termination, any classified contracts or sub-contracts shall continue to be treated in accordance with the provisions of this Agreement unless otherwise agreed by the Parties.

IN WITNESS WHEREOF, the undersigned, being duly authorised thereto by their respective Governments have signed this Agreement.

Done in duplicate at Madrid this 16th day of December 2019 in the Spanish and English languages, both texts being equally authoritative.

For the Kingdom of Spain



FERNANDO VALENZUELA MARZO

Secretary of State for Foreign Affairs

For New Zealand

FLETCHER TABUTEAU

Parliamentary Under-Secretary for Foreign Affairs

ANNEX A to the Agreement between the Kingdom of Spain and the Government of New Zealand relating to the Protection of Classified Information 16th December 2019

REQUEST FOR VISITS

The request for visits must contain the following information:

a) Full name of the visitor, date and place of birth, nationality and passport (or other relevant identity document) number;

b) Employment and duties of the visitor, name of the establishment of the organisation which employs them;

c) Level and date of expiry of the visitor's PSC ;

d) Proposed date of the visit and anticipated duration;

e) Purpose of the visit and any useful indications on the subject to be treated and the levels of classification for the classified information;

f) Name of establishments, installations and localities, purposes of the visit;

g) Full names of persons who should receive the visitor, if possible;

h) Date, signature and appenditure of the authorised official stamp (of security).

[SPANISH TEXT – TEXTE ESPAGNOL]

ACUERDO

ENTRE

EL REINO DE ESPAÑA

Y

EL GOBIERNO DE NUEVA ZELANDA

RELATIVO A

LA PROTECCIÓN DE INFORMACIÓN CLASIFICADA

El Reino de España

y

el Gobierno de Nueva Zelanda,

en lo sucesivo denominados las "Partes",

Interesados en proteger la información clasificada en el ámbito de la defensa;

Deseosos de establecer las condiciones para la protección de la información y material clasificada en el ámbito de la defensa que las Partes intercambien o elaboren, incluidas las disposiciones para el intercambio con entidades públicas o privadas de conformidad con las leyes y los reglamentos nacionales correspondientes de las Partes,

han convenido en lo siguiente:

ARTÍCULO 1
DEFINICIONES

A efectos del presente Acuerdo,

Por "**contrato clasificado**" se entenderá un contrato, subcontrato o proyecto que exija acceso a información clasificada o pueda generarla.

Por "**información clasificada**" se entenderá aquella información generada por el Reino de España o el Gobierno de Nueva Zelanda, o en su nombre, o que se halle bajo la jurisdicción o el control de uno de ellos, y requiera protección para la seguridad nacional y haya sido designada como tal mediante la concesión de una clasificación de seguridad acorde a las leyes y los reglamentos nacionales de la Parte o de las Partes. La información podrá ser verbal, visual, electrónica o documental, o en forma de material, incluidos equipos o tecnología.

Por "**Autoridad de Seguridad Competente**" o "**ASC**" se entenderá la autoridad designada de conformidad con la legislación del Gobierno del Estado responsable, en última instancia, de aplicar las disposiciones del presente Acuerdo y transmitir la información clasificada a la otra Parte.

Por "**Contratista**" se entenderá la persona física o jurídica con capacidad legal de otorgar contratos.

Por "**Habilitación de Seguridad de Establecimiento**" o "**HSES**" se entenderá la determinación, por la ASC de una Parte, de que el Contratista cuenta con medidas de seguridad adecuadas en un establecimiento concreto para proteger la información clasificada hasta un grado de clasificación de seguridad concreto, éste incluido.

Por "**Parte Anfitriona**" se entenderá aquella Parte en cuyo territorio se produce la visita.

Por "**necesidad de conocer**" se entenderá la necesidad de acceder a información clasificada en el marco de una función oficial reconocida con un fin autorizado específico.

Por "**Parte de Origen**" se entenderá la Parte que cree, entregue o transmita información clasificada a la Parte Receptora.

Por "**Usuario de Origen**" se entenderá la persona, agencia u organización, pública o privada, contratada o autorizada por la Parte de Origen para crear, entregar o transmitir información clasificada en su nombre.

Por "**Habilitación Personal de Seguridad**" o "**HPS**" se entenderá la determinación, por la ASC de una Parte, de que una persona física ha sido habilitada para acceder a información clasificada, y manejarla hasta un grado de clasificación de seguridad concreto, éste incluido, de conformidad con sus leyes y reglamentos nacionales.

Por "**Parte Receptora**" se entenderá la Parte que reciba la información clasificada transmitida por la Parte de Origen.

Por "**Usuario Receptor**" se entenderá la persona, agencia u organización, pública o privada, contratada o autorizada por la Parte Receptora para manejar información clasificada en su nombre.

Por "**grado de clasificación de seguridad**" se entenderá la categoría asignada a la información clasificada, con indicación de su confidencialidad, del grado de perjuicio que puede desprenderse en caso de divulgación no autorizada o pérdida, y del grado de protección que deben aplicar las Partes.

Por "**incidente de seguridad**" se entenderá todo acto u omisión contrario a las leyes y los reglamentos nacionales que puedan resultar o resulten en el acceso o la divulgación no autorizados, la pérdida, la destrucción o comprometimiento de la información clasificada que haya sido generada y/o intercambiada en virtud del presente Acuerdo.

Por "**Tercero**" se entenderá cualquier Estado, incluidas las personas jurídicas y físicas sujetas a su jurisdicción, u organización internacional que no sea Parte en el presente Acuerdo.

ARTÍCULO 2
OBJETO

El presente Acuerdo regula el intercambio de toda la información clasificada en materia de defensa entre las Partes, o entre entidades públicas o privadas sin perjuicio de sus leyes y reglamentos nacionales.

ARTÍCULO 3
AUTORIDADES DE SEGURIDAD COMPETENTES

1. Las Autoridades de Seguridad Competentes responsables del control general y de la aplicación del presente Acuerdo son:
   a. **Para el Reino de España:**
      Secretario de Estado Director del Centro Nacional de Inteligencia
      Oficina Nacional de Seguridad

   b. **Para Nueva Zelanda:**
      Director General
      Servicio de Inteligencia de Seguridad, Nueva Zelanda

2. Las Partes se informarán mutuamente por escrito de todos los cambios que se produzcan en la designación de las ASC. Dichos cambios no constituirán una modificación formal del presente Acuerdo.

ARTÍCULO 4
DISPOSICIONES EN MATERIA DE SEGURIDAD

1. De conformidad con sus leyes y reglamentos nacionales, las Partes adoptarán las medidas adecuadas para proteger la información clasificada que se transmita, reciba o genere con sujeción a las condiciones del presente Acuerdo y le otorgarán un grado de protección equivalente al que otorgan a su propia información clasificada nacional, de conformidad con la definición prevista en el artículo 5.

2. La protección de la información clasificada intercambiada entre las Partes se regirá por los siguientes principios:

   a) La Parte Receptora otorgará a la información clasificada que reciba un grado de protección equivalente al que la Parte de Origen aplica expresamente, de conformidad con la equivalencia que se establece en el artículo 5 del presente Acuerdo.

   b) El acceso a la información clasificada se limita solamente a las personas que hayan recibido la autorización previa para el grado requerido y cuyas funciones requieran dicho acceso ateniéndose a la necesidad de conocer.

   c) La Parte Receptora no transmitirá información clasificada a ningún Tercero sin el consentimiento previo por escrito de la ASC de la Parte de Origen.

   d) La información clasificada no podrá utilizarse con fines distintos de aquellos para los que se transmitió oficialmente.

   e) Cuando una Parte de Origen modifique la clasificación de la información clasificada intercambiada de conformidad con el presente Acuerdo, comunicará por escrito dicho cambio a la otra Parte.

   f) La Parte Receptora no rebajará el grado de la información clasificada ni la desclasificará sin la autorización previa por escrito de la ASC de la Parte de Origen.

3. De conformidad con el procedimiento recogido en el presente Acuerdo, previa petición, las ASC, o los representantes autorizados de cada una de las Partes, visitarán las sedes e instalaciones en el territorio de la otra Parte para examinar las medidas de protección adoptadas con el fin de garantizar la seguridad de la información clasificada que se transmita según lo aquí dispuesto.

ARTÍCULO 5
CLASIFICACIONES DE SEGURIDAD EQUIVALENTES

1. Las Partes, habiendo tomado nota de las medidas de seguridad que prevén sus leyes y reglamentos nacionales respectivos, se comprometen a velar por la protección de la información clasificada y adoptar el grado equivalente de clasificación de seguridad establecido en el siguiente cuadro:

ESPAÑA	NUEVA ZELANDA
SECRETO	TOP SECRET
RESERVADO	SECRET
CONFIDENCIAL	CONFIDENTIAL
DIFUSIÓN LIMITADA	RESTRICTED

2. Las clasificaciones de seguridad de las Partes se aplican como sigue:

Para la información clasificada española:

SECRETO, la divulgación no autorizada o el uso indebido pondría en peligro o supondría un perjuicio extremadamente grave para los intereses nacionales;
RESERVADO, la divulgación no autorizada o el uso indebido pondría en peligro o supondría un grave perjuicio para los intereses nacionales;
CONFIDENCIAL, la divulgación no autorizada o el uso indebido pondría en peligro o supondría un perjuicio para los intereses nacionales;
DIFUSIÓN LIMITADA, la divulgación no autorizada o el uso indebido podría ser contrario a los intereses nacionales.

Para la información clasificada neozelandesa:

TOP SECRET, el comprometimiento de la información perjudicaría de manera extremadamente grave los intereses nacionales;
SECRET, el comprometimiento de la información perjudicaría gravemente los intereses nacionales;
CONFIDENTIAL, el comprometimiento de la información perjudicaría de manera importante los intereses nacionales;
RESTRICTED, el comprometimiento de la información perjudicaría de manera negativa los intereses nacionales.

3. Las Partes se mantendrán informadas mutuamente por escrito de los cambios en sus correspondientes leyes y reglamentos nacionales en materia de protección de información clasificada.

ARTÍCULO 6
HABILITACIÓN PERSONAL DE SEGURIDAD

1. Las personas físicas no tendrán derecho a acceder a la información clasificada solamente en virtud de su rango, cargo o HPS.

2. Para acceder a la información clasificada con grado CONFIDENCIAL / CONFIDENTIAL o superior, cada una de las Partes, de conformidad con sus leyes y reglamentos nacionales, se cerciorará de que la persona que tenga acceso a la misma, o pueda requerirlo, de conformidad con el presente Acuerdo, cuenta con una habilitación de seguridad de grado igual o superior a la información a la que se accede.

3. Cuando sea necesario, las ACS de cada Parte prestarán su ayuda en la concesión de una HPS o, notificarán oportunamente los datos de la HPS de un ciudadano de una Parte que resida en el territorio de la otra Parte y requiera acceso a información clasificada.

4. No se precisa HPS para acceder a información clasificada del grado DIFUSIÓN LIMITADA / RESTRICTED. El acceso a la misma se limitará a personas físicas que tengan la necesidad de conocer y hayan sido informadas de sus responsabilidades y obligaciones de protegerla.

ARTÍCULO 7
DIVULGACIÓN

1. La información clasificada que intercambien, transmitan o generen juntas ambas Partes en virtud del presente Acuerdo, incluidos contratos u otras actividades de cooperación, no podrá ser rebajada de grado, desclasificada o transmitida a ningún Tercero, sin autorización previa por escrito de la Parte de Origen.

2. En el ámbito de aplicación de las leyes y los reglamentos nacionales, la Parte Receptora adoptará todas las medidas razonables a su disposición para evitar la divulgación de la información clasificada. Si se solicita la divulgación de cualquier información clasificada facilitada en virtud del presente Acuerdo, la Parte Receptora se lo notificará de inmediato por escrito a la Parte de Origen y ambas se consultarán entre sí por esta misma vía antes de que la Parte Receptora se pronuncie al respecto.

ARTÍCULO 8
COOPERACIÓN EN MATERIA DE SEGURIDAD

1. Cuando la ASC de una Parte solicite confirmación de la HSES de un Contratista de la otra Parte o de la HPS de una persona física de la misma, cursará formalmente petición escrita a la ASC de dicha Parte.

2. Cuando reciba dicha solicitud, la ASC notificará a la ASC solicitante la situación de la HSES o de la HPS del Contratista o persona física correspondiente, así como la validez de la HSES o la fecha de vencimiento de la HPS.

3. Las ASC colaborarán en la ejecución de las investigaciones en materia de seguridad relativas a la HSES o la HPS, previa petición y de conformidad con las leyes y los reglamentos nacionales.

4. Si, de conformidad con las leyes y los reglamentos nacionales, la ASC revoca o rebaja de grado una HSES o HPS vigente expedida a favor de un Contratista o una persona física que hayan sido confirmados, se notificará por escrito a la ASC de la otra Parte a la mayor brevedad.

ARTÍCULO 9
REPRODUCCIÓN, TRADUCCIÓN Y DESTRUCCIÓN

1. Cuando se reciban las reproducciones o traducciones de los originales, la Parte Receptora los marcará en consonancia como tales y se conferirá a dichos documentos el mismo grado de protección que al original.

2. Las traducciones incorporarán una anotación adecuada en el idioma de la traducción en la que se mencionará la existencia de información clasificada de la otra Parte.

3. Las traducciones y reproducciones se limitarán a las mínimas necesarias con fines oficiales y serán realizadas exclusivamente por personas físicas con necesidad de conocer y titulares de una HPS del grado de clasificación de seguridad de la información clasificada objeto de reproducción o traducción.

4. La información clasificada con grado SECRETO / TOP SECRET solo podrá traducirse o reproducirse con el previo consentimiento por escrito de la ASC de la Parte de Origen.

5. La información clasificada se destruirá según las normas al efecto recogidas en las leyes y los reglamentos nacionales de la Parte correspondiente.

6. Cuando la Parte Receptora haya destruido un documento o información clasificada, expedirá y facilitará a la Parte de Origen un certificado de destrucción.

7. La información clasificada con grado SECRETO / TOP SECRET no podrá destruirse. Será devuelta a la Parte de Origen.

8. Si, debido a una situación crítica, fuera imposible proteger la información clasificada facilitada en virtud del presente Acuerdo, se destruirá a la mayor brevedad posible por los medios adecuados para evitar un incidente de seguridad. La Parte Receptora notificará por escrito a la ASC de la Parte de Origen de la necesidad de destruir la información clasificada con grado RESERVADO / SECRET en caso de situación crítica.

ARTÍCULO 10
TRANSMISIÓN DE LA INFORMACIÓN A LOS USUARIOS

1. El presente artículo es de aplicación en caso de transmisión de información clasificada:

   a) de la Parte de Origen al Usuario Receptor a través de la Parte Receptora;

   b) cuando así lo hayan pactado de mutuo acuerdo la Parte de Origen y la Parte Receptora, de la Parte de Origen directamente al Usuario Receptor; y

   c) cuando así lo hayan pactado de mutuo acuerdo la Parte de Origen y la Parte Receptora, del Usuario de Origen directamente al Usuario Receptor.

2. Antes de recibir la información clasificada (tanto si el destinatario es la Parte Receptora como el Usuario Receptor), la ASC de la Parte Receptora:

   a) garantizará que sus instalaciones disponen de la HSES oportuna;

   b) garantizará que las personas físicas que vayan a tener acceso a información clasificada se encuentran en posesión de la HPS correspondiente;

   c) garantizará que se informa a todas las personas que tengan acceso a información clasificada de las responsabilidades que les atribuyen las leyes y los reglamentos nacionales; y

   d) garantizará que se confirma por escrito a la mayor brevedad la recepción de la información clasificada a la Parte de Origen.

ARTÍCULO 11
TRANSMISIÓN ENTRE LAS PARTES

1. La transmisión de información clasificada entre las Partes se enviará normalmente por conducto diplomático, o por los cauces que convengan de mutuo acuerdo, de conformidad con las leyes y los reglamentos nacionales de la Parte de Origen.

2. Las transmisiones cumplirán las siguientes prescripciones:

   a) La Parte de Origen se cerciorará de que la persona física que transmita la información:

      i. es un empleado público o empleado suyo o del Usuario de Origen, y
      ii. se encuentra en posesión de una HPS, al menos, de igual grado que la información clasificada objeto de transmisión.

   b) La persona que remita la información clasificada deberá trasladar una carta de la ASC que indique:

      i. la autorización concedida a la persona física para trasladar información clasificada;
      ii. el punto de contacto de la Parte de Origen; y
      iii. el punto de contacto de la Parte Receptora.

c) La Parte de Origen llevará un registro de la información clasificada transmitida, del que facilitará copia a la Parte Receptora previa petición. Ambas Partes pondrán en conocimiento de sus ASC los detalles del registro.

d) La información clasificada se empaquetará y sellará adecuadamente, de conformidad con las leyes y los reglamentos nacionales de la Parte de Origen.

3. La información clasificada sólo podrá transmitirse por vía electrónica en formato cifrado, utilizando para ello los métodos y equipos de cifra que fijen de mutuo acuerdo las ASC correspondientes.

ARTÍCULO 12
CONTRATOS CLASIFICADOS

1. Si la ASC de una de las Partes, o un Contratista sujeto a su jurisdicción, propone otorgar un contrato clasificado con información clasificada de grado CONFIDENCIAL / CONFIDENTIAL, o superior, con un Contratista sujeto a la jurisdicción de la otra Parte, obtendrá primero por escrito de la ASC de la otra Parte, con arreglo al artículo 8 del Acuerdo, la confirmación de que dicho Contratista dispone de una HSES y/o HPS del grado de clasificación de seguridad oportuno.

2. La ASC que haya otorgado la HSES o HPS será responsable de garantizar que, en materia de seguridad, el Contratista se atiene a las leyes y los reglamentos nacionales.

3. Los contratos clasificados que se limitan a información clasificada con grado DIFUSIÓN LIMITADA / RESTRICTED no requieren HSES o HPS.

4. Los contratos o subcontratos que contengan información clasificada incorporarán estipulaciones referentes a la protección de la misma, que dotarán de efecto a las disposiciones del presente Acuerdo y otras condiciones referentes al uso de información clasificada que imponga la Parte de Origen, que será la única facultada para modificar el grado de clasificación de la información o autorizar su nueva divulgación.

5. La ASC de la Parte de Origen transmitirá copia de las disposiciones en materia de seguridad contenidas en los contratos a la ASC de la Parte Receptora.

ARTÍCULO 13
VISITAS

1. Las visitas de ciudadanos de una Parte a la ubicación de la otra Parte donde se custodia información clasificada están permitidas a condición de que la ASC de la Parte Anfitriona lo haya aprobado previamente por escrito. Las visitas de ciudadanos de terceros Estados a zonas en las que las Partes intercambien información clasificada únicamente podrán realizarse con el consentimiento mutuo de ambas.

2. Las solicitudes de visita se elevarán por conducto diplomático a la ASC de la Parte Anfitriona con una antelación mínima de tres semanas a la fecha de la visita y recogerán la información que se especifica el Anexo A al presente Acuerdo.

3. El periodo máximo por el que las Partes podrán solicitar un permiso de visita será de doce meses. Si una visita concreta no pudiera concluirse en el periodo indicado en la autorización a tal efecto, o si se requiere una prórroga del periodo para el que se concede la autorización de acceso, la Parte solicitante podrá solicitar una nueva visita autorizada, siempre que lo haga al menos tres semanas antes de que expire la autorización vigente.

4. Todos los visitantes deben cumplir con las leyes y los reglamentos nacionales de la Parte Anfitriona en materia de protección de información clasificada.

5. Solamente se autorizarán las visitas si la persona física dispone de la HPS oportuna y tiene necesidad de conocer.

ARTÍCULO 14
VISITAS MÚLTIPLES

1. Para cualquier proyecto, programa o contrato clasificado, las Partes podrán confeccionar listas de personal autorizado a efectuar múltiples visitas, de conformidad con las condiciones que acuerden sus ASC. Estas visitas tendrán una validez inicial de doce meses, que podrá prolongarse por acuerdo de las ASC por nuevos periodos que no excederán de doce meses en total.

2. Cuando la ASC anfitriona haya aprobado dicha lista, los establecimientos correspondientes podrán acordar directamente los pormenores de las visitas.

ARTÍCULO 15
INCIDENTES DE SEGURIDAD

1. Si se sospecha o se confirma que se ha producido un incidente de seguridad relacionado con información clasificada de la otra Parte, la Parte en la que el incidente se ha producido lo investigará e informará inmediatamente por escrito a la ASC de la otra Parte.

2. La notificación deberá ser lo suficientemente detallada, de tal manera que permita a la Parte de Origen iniciar una evaluación completa de las consecuencias.

3. La Parte Receptora abrirá una investigación (con ayuda de la otra Parte, si fuera necesario) y adoptará todas las medidas adecuadas, de conformidad con sus leyes y reglamentos nacionales, para limitar las consecuencias. La Parte Receptora comunicará a la Parte de Origen los resultados de la investigación y todas las medidas tomadas para evitar que vuelva a suceder.

ARTÍCULO 16
COSTES

En caso de que se produzca algún gasto, cada Parte se hará cargo de aquellos propios relacionados con las actividades realizadas de conformidad con el presente Acuerdo.

ARTÍCULO 17
SOLUCIÓN DE CONTROVERSIAS

Las Partes resolverán exclusivamente mediante consulta toda controversia en torno a la interpretación o aplicación del presente Acuerdo.

ARTÍCULO 18
DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL

Nada de lo dispuesto en el presente Acuerdo se entenderá que merma o limita la propiedad intelectual e industrial (incluidas patentes y derechos de autor) asociada a la información clasificada transmitida sobre la que cualquiera de las Partes, sus Contratistas o Terceros puedan tener derechos.

ARTÍCULO 19
DISPOSICIONES FINALES

1. Las Partes se notificarán por escrito la conclusión de los procedimientos internos que sean necesarios para que el presente Acuerdo entre en vigor, lo que se producirá el día en que se reciba la segunda notificación.

2. El presente Acuerdo podrá modificarse en su momento con el consentimiento mutuo por escrito de las Partes. Las modificaciones entrarán en vigor siguiendo el mismo procedimiento descrito en el apartado 1 del presente artículo.

3. El Anexo forma parte integrante del Acuerdo.

4. Las ASC podrán formalizar acuerdos administrativos para la ejecución del presente Acuerdo.

5. El presente Acuerdo permanecerá en vigor durante un periodo de tiempo indefinido. Cualquiera de las Partes podrá terminarlo cursando notificación escrita por conducto diplomático a la otra Parte con seis meses de antelación.

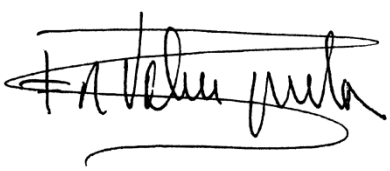
6. Las obligaciones en materia de protección de información clasificada intercambiada al amparo del Acuerdo se mantendrán vigentes sin perjuicio de la terminación del mismo.

7. En caso de terminación, seguirá dispensándose a los contratos o subcontratos clasificados un tratamiento acorde a las disposiciones del presente Acuerdo, salvo pacto en contrario de las Partes.

EN FE DE LO CUAL, los abajo firmantes, debidamente autorizados por sus respectivos Gobiernos, firman el presente Acuerdo.

Hecho en duplicado en Madrid el día 16 de diciembre de 2019, en lengua española e inglesa, siendo ambos textos igualmente auténticos.

Por el Reino de España



FERNANDO VALENZUELA MARZO

Secretario de Estado de Asuntos Exteriores

Por Nueva Zelanda

FLETCHER TABUTEAU

Viceministro Parlamentario de Asuntos Exteriores

ANEXO A al Acuerdo entre el Reino de España y el Gobierno de Nueva Zelanda relativo a la protección de información clasificada 16 de diciembre de 2019

SOLICITUD DE VISITA

Las solicitudes de visita deben contener la siguiente información:

a) nombre completo del visitante, fecha y lugar de nacimiento, nacionalidad y número de pasaporte (u otro documento de identidad pertinente);

b) cargo y funciones del visitante, nombre del establecimiento de la organización en la que trabaja;

c) grado y fecha de vencimiento de la HPS del visitante;

d) fecha propuesta para la visita y duración prevista;

e) propósito de la visita e indicaciones de interés sobre el asunto a tratar y los grados de clasificación de la información clasificada;

f) nombre de los establecimientos, instalaciones y emplazamiento, así como fines de la visita;

g) nombre completo de las personas que deben recibir al visitante, cuando sea posible;

h) fecha, firma y sello oficial autorizado (de seguridad).

[TRANSLATION – TRADUCTION]

ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LE GOUVERNEMENT DE NOUVELLE-ZÉLANDE RELATIF À LA PROTECTION D'INFORMATIONS CLASSIFIÉES

Le Royaume d'Espagne

et

le Gouvernement de la Nouvelle-Zélande,

Ci-après dénommés « les Parties »,

Ayant un intérêt à ce que les informations classifiées en matière de défense soient protégées,

Désireux d'établir les conditions de protection des informations et du matériel classifiés en matière de défense échangés ou élaborés par les Parties, notamment les dispositions relatives à l'échange avec des organismes publics ou privés, conformément à la législation et réglementation internes applicables des Parties,

Sont convenus de ce qui suit

ARTICLE PREMIER. DÉFINITIONS

Aux fins du présent Accord :

le terme « contrat classifié » désigne un contrat, un contrat de sous-traitance ou un projet pour lesquels l'accès à des informations classifiées est requis ou dans le cadre desquels des informations classifiées sont susceptibles d'être créées ;

le terme « informations classifiées » désigne les informations qui sont créées par ou pour le Royaume d'Espagne ou le Gouvernement de la Nouvelle-Zélande, ou qui sont placées sous la juridiction ou le contrôle de l'un d'entre eux, et qui nécessitent d'être protégées dans l'intérêt de la sécurité nationale et qui sont ainsi désignées par l'attribution d'une classification de sécurité conformément aux lois et règlements internes de la ou les Parties. Les informations peuvent être présentées sous forme orale, visuelle, électronique ou documentaire, ou sous la forme de matériel, y compris d'équipement ou de technologie ;

le terme « autorité de sécurité compétente » désigne l'autorité désignée en vertu de la loi du Gouvernement de l'État qui est responsable en dernier ressort de la mise en œuvre des dispositions du présent Accord et de la transmission d'informations classifiées à l'autre Partie ;

le terme « contractant » désigne toute personne physique ou morale ayant la capacité juridique de conclure des contrats ;

le terme « habilitation de sécurité d'établissement » désigne une décision prise par l'autorité de sécurité compétente d'une Partie selon laquelle, du point de vue de la sécurité, un établissement spécifié peut assurer la protection d'informations classifiées jusqu'à un certain niveau de classification de sécurité, le contractant ayant mis en place les mesures de sûreté appropriées ;

le terme « Partie hôte » désigne la Partie sur le territoire de laquelle une visite a lieu ;

le terme « besoin d'en connaître » désigne la nécessité d'accéder à des informations classifiées dans le cadre d'une fonction officielle reconnue et à des fins autorisées spécifiques ;

le terme « Partie d'origine » désigne la Partie qui crée, fournit ou transmet des informations classifiées à la Partie destinataire ;

le terme « utilisateur d'origine » désigne une personne physique ou morale, une agence ou une organisation qui est engagée ou autorisée par la Partie d'origine à créer, à fournir ou à transmettre des informations classifiées pour la Partie d'origine ;

le terme « habilitation de sécurité personnelle » désigne une habilitation délivrée à une personne par l'autorité de sécurité compétente, conformément à ses lois et règlements, en vertu de laquelle ladite personne est autorisée à manipuler des informations classifiées jusqu'à un certain niveau de classification de sécurité ou à en prendre connaissance ;

le terme « Partie destinataire » désigne la Partie qui reçoit des informations classifiées transmises par la Partie d'origine ;

le terme « utilisateur destinataire » désigne une personne physique ou morale, une agence ou une organisation qui est engagée ou autorisée par la Partie destinataire à manipuler des informations classifiées pour la Partie destinataire ;

le terme « niveau de classification de sécurité » désigne une catégorie attribuée aux informations classifiées qui indique leur niveau de sensibilité, l'ampleur des dommages qui pourraient survenir en cas de divulgation ou de perte non autorisée et le niveau de protection que les Parties doivent assurer ;

le terme « incident de sécurité » désigne un acte ou une omission contraire aux lois et règlements internes qui peut entraîner ou entraîne l'accès non autorisé, la divulgation, la perte, la destruction ou la compromission d'informations classifiées qui ont été créées ou échangées dans le cadre du présent Accord ;

le terme « tierce partie » désigne tout État, y compris les personnes physiques et morales placées sous sa juridiction, ou toute organisation internationale, qui n'est pas partie au présent Accord.

ARTICLE 2. CHAMP D'APPLICATION

Le présent Accord régit l'échange de toutes les informations classifiées relatives aux questions de défense entre les Parties ou entre des organismes publics ou privés, sous réserve de leurs lois et règlements internes.

ARTICLE 3. AUTORITÉS COMPÉTENTES DE SÉCURITÉ

1. Les autorités de sécurité compétentes responsables du contrôle général et de la mise en œuvre du présent Accord sont :

a. Pour le Royaume d'Espagne :

le Secrétaire d'État, Directeur du Centre national du renseignement, Bureau de sécurité nationale

b. Pour la Nouvelle-Zélande :

le Directeur général,

Service néo-zélandais du renseignement de sécurité

2. Les Parties se tiennent mutuellement informées par écrit de toute modification apportée à la nomination de leur autorité de sécurité compétente. Ladite modification n'est pas considérée comme une modification officielle au présent Accord.

ARTICLE 4. PRINCIPES DE SÉCURITÉ

1. Conformément à leurs lois et règlements internes, les Parties prennent les mesures appropriées afin de protéger les informations classifiées qui sont transmises, reçues ou créées dans le cadre du présent Accord et offrent auxdites informations un niveau de protection équivalent à celui qu'elles accordent à leurs propres informations classifiées nationales, tel que défini à l'article 5.

2. La protection des informations classifiées échangées entre les Parties est régie par les principes suivants :

a) la Partie destinataire attribue aux informations classifiées qu'elle reçoit un niveau de protection équivalent à celui expressément appliqué auxdites informations par la Partie d'origine, conformément au tableau des équivalences établi à l'article 5 du présent Accord ;

b) l'accès aux informations classifiées est limité aux personnes qui ont reçu une autorisation préalable pour le niveau requis et dont les fonctions exigent l'accès auxdites informations classifiées sur la base du besoin d'en connaître ;

c) la Partie destinataire ne transmet pas d'informations classifiées à une tierce partie sans l'accord écrit préalable de l'autorité de sécurité compétente de la Partie d'origine ;

d) les informations classifiées ne peuvent être utilisées à des fins autres que celles pour lesquelles elles sont officiellement transmises ;

e) lorsqu'une Partie d'origine modifie la classification de toute information classifiée échangée dans le cadre du présent Accord, elle en informe l'autre Partie par écrit ;

f) la Partie destinataire ne doit pas déclasser ou déclassifier les informations classifiées transmises sans l'accord écrit préalable de l'autorité de sécurité compétente de la Partie d'origine.

3. Conformément aux procédures prévues par le présent Accord, les autorités de sécurité compétentes de chaque Partie ou leurs représentants agréés peuvent visiter, sur demande, les sites et installations situés sur le territoire de l'autre Partie pour examiner les mesures de protection mises en place pour assurer la sécurité des informations classifiées qui sont transmises en application du présent Accord.

ARTICLE 5. ÉQUIVALENCE DES NIVEAUX DE CLASSIFICATIONS DE SÉCURITÉ

1. Les Parties, compte tenu des mesures de sûreté prescrites par leurs lois et règlements internes respectifs, s'engagent à assurer la protection des informations classifiées échangées et adoptent le niveau équivalent de classifications de sécurité tel que défini dans le tableau ci-dessous :

ESPAGNE	**NOUVELLE-ZÉLANDE**
SECRETO	TOP SECRET (TRÈS SECRET)

ESPAGNE	NOUVELLE-ZÉLANDE
RESERVADO	SECRET (SECRET)
CONFIDENCIAL	CONFIDENTIAL (CONFIDENTIEL)
DIFUSION LIMITADA	RESTRICTED (RESTREINT)

2. Les classifications de sécurité des Parties sont appliquées comme suit :

Pour les informations classifiées espagnoles :

SECRETO : la divulgation non autorisée ou la mauvaise utilisation des informations risquerait de compromettre ou de causer un préjudice extrêmement grave aux intérêts nationaux ;

RESERVADO : la divulgation non autorisée ou la mauvaise utilisation des informations risquerait de compromettre ou de nuire gravement aux intérêts nationaux ;

CONFIDENCIAL : la divulgation non autorisée ou la mauvaise utilisation des informations risquerait de compromettre ou de nuire aux intérêts nationaux ;

DIFUSIÓN LIMITADA : une divulgation non autorisée ou une mauvaise utilisation des informations qui irait à l'encontre des intérêts nationaux.

Pour les informations classifiées néo-zélandaises :

TOP SECRET : la compromission d'informations causerait un préjudice extrêmement grave aux intérêts nationaux ;

SECRET : la compromission d'informations nuirait gravement aux intérêts nationaux ;

CONFIDENTIAL : la compromission d'informations porterait préjudice aux intérêts nationaux ;

RESTRICTED : la compromission d'informations porterait préjudice aux intérêts nationaux d'une manière défavorable.

3. Les Parties s'informent par écrit de toute modification apportée à leurs lois et règlements internes respectifs en matière de protection des informations classifiées.

ARTICLE 6. HABILITATION DE SECURITÉ PERSONNELLE

1. Nul ne peut avoir accès à des informations classifiées uniquement en raison de son rang, de son poste ou d'une habilitation de sécurité personnelle.

2. Pour l'accès aux informations classifiées CONFIDENCIAL/CONFIDENTIAL ou d'une classification supérieure, chaque Partie veille, conformément à ses lois et règlements internes, à ce que chaque personne qui a accès aux informations classifiées ou qui peut en exiger l'accès en vertu du présent Accord, détienne une habilitation de sécurité correspondant au niveau de classification des informations consultées ou supérieur.

3. L'autorité de sécurité compétente de chaque Partie aide, lorsque cela est nécessaire, à la délivrance d'une habilitation de sécurité personnelle ou d'une notification appropriée à un ressortissant d'une Partie résidant sur le territoire de l'autre Partie et exigeant l'accès à des informations classifiées.

4. Aucune habilitation de sécurité personnelle n'est requise pour l'accès aux informations classifiées de niveau DIFUSIÓN LIMITADA/RESTRICTED. Ledit accès est limité aux personnes

physiques qui ont un besoin d'en connaître et qui ont été dûment informées de leurs responsabilités et obligations en matière de protection desdites informations classifiées.

ARTICLE 7. DIVULGATION

1. Les informations classifiées échangées, transmises ou produites conjointement par les deux Parties dans le cadre du présent Accord, y compris les contrats ou toute autre activité de coopération, ne peuvent être déclassées, déclassifiées ou transmises à une tierce partie sans l'accord écrit préalable de la Partie d'origine.

2. Dans le cadre de ses lois et règlements internes, la Partie destinataire prend toutes les mesures raisonnables à sa disposition pour empêcher la divulgation d'informations classifiées. En cas de demande de divulgation de toute information classifiée fournie en vertu du présent Accord, la Partie destinataire en informe immédiatement la Partie d'origine par écrit, et les deux Parties se consultent par écrit avant qu'une décision de divulgation ne soit prise par la Partie destinataire.

ARTICLE 8. COOPÉRATION EN MATIÈRE DE SÉCURITÉ

1. Lorsque l'autorité de sécurité compétente d'une Partie demande la confirmation de l'habilitation de sécurité d'établissement d'un contractant de l'autre Partie ou de l'habilitation de sécurité personnelle d'une personne physique de l'autre Partie, elle présente une demande écrite officielle à l'autorité de sécurité compétente de ladite Partie.

2. Dès réception d'une telle demande, l'autorité de sécurité compétente notifie à l'autorité de sécurité compétente requérante le statut de l'habilitation de sécurité d'établissement ou de l'habilitation de sécurité personnelle du contractant concerné ou de la personne concernée ainsi que la durée de validité de l'habilitation de sécurité d'établissement ou la date d'expiration de l'habilitation de sécurité personnelle.

3. Les autorités de sécurité compétentes se prêtent mutuellement assistance pour mener des enquêtes de sécurité relatives aux habilitations de sécurité d'établissement et aux habilitations de sécurité personnelle sur demande et conformément aux lois et règlements internes des Parties.

4. Si, conformément aux lois et règlements internes des Parties, une autorité de sécurité compétente retire ou déclasse une habilitation de sécurité d'établissement ou une habilitation de sécurité personnelle existante délivrée à un contractant ou à une personne physique pour lesquels une confirmation a été fournie, l'autorité de sécurité compétente de l'autre Partie en est avisée par écrit dès que possible.

ARTICLE 9. REPRODUCTION, TRADUCTION ET DESTRUCTION

1. Dès réception de reproductions ou de traductions d'originaux, la Partie destinataire les marque en tant que reproductions ou traductions. Il convient d'accorder à ces documents la même protection qu'au document original.

2. Les traductions contiennent une annotation appropriée, dans la langue de traduction, indiquant qu'elles contiennent des informations classifiées de l'autre Partie.

3. Les traductions et les reproductions sont limitées au minimum requis à des fins officielles et ne sont réalisées que par des personnes ayant un besoin d'en connaître et qui détiennent une habilitation de sécurité personnelle correspondant au niveau de classification de sécurité des informations classifiées reproduites ou traduites.

4. Les informations classifiées de niveau SECRETO/TOP SECRET ne sont traduites ou reproduites qu'avec le consentement écrit préalable de l'autorité de sécurité compétente de la Partie d'origine.

5. Les informations classifiées sont détruites conformément aux normes de destruction prescrites par les lois et règlements internes des Parties respectives.

6. Lors de la destruction d'un document ou d'informations classifiés par la Partie destinataire, cette dernière doit être en possession d'un certificat écrit de destruction et le remettre à la Partie d'origine.

7. Les informations classifiées SECRETO/TOP SECRET ne sont pas détruites. Elles sont restituées à la Partie d'origine.

8. Si une situation de crise rend impossible la protection d'informations classifiées communiquées au titre du présent Accord, celles-ci sont détruites dès que possible par tout moyen approprié pour éviter un incident de sécurité. La Partie destinataire notifie par écrit à l'autorité de sécurité compétente de la Partie d'origine la nécessité de détruire, en cas de situation de crise, les informations classifiées de niveau RESERVADO/SECRET ou d'une classification supérieure fournies en vertu du présent Accord.

ARTICLE 10. COMMUNICATION D'INFORMATIONS AUX UTILISATEURS

1. Le présent article s'applique aux cas de transmission d'informations classifiées :
   a) de la Partie d'origine à l'utilisateur destinataire par l'intermédiaire de la Partie destinataire ;
   b) lorsqu'il y a accord mutuel entre la Partie d'origine et la Partie destinataire, de la Partie d'origine à l'utilisateur destinataire ;
   c) lorsqu'il y a accord mutuel entre la Partie d'origine et la Partie destinataire, de l'utilisateur d'origine à l'utilisateur destinataire.

2. Avant la réception d'informations classifiées (peu importe que le destinataire soit la Partie destinataire ou l'utilisateur destinataire), l'autorité de sécurité compétente de la Partie destinataire doit :
   a) veiller à ce que ses établissements soient en possession de l'habilitation de sécurité d'établissement appropriée ;
   b) veiller à ce que les personnes physiques qui auront accès aux informations classifiées soient en possession de l'habilitation de sécurité personnelle appropriée ;
   c) veiller à ce que toutes les personnes qui ont accès aux informations classifiées soient informées de leurs responsabilités qui découlent des lois et règlements internes des Parties ;
   d) veiller à ce que la réception des informations classifiées soit confirmée par écrit à la Partie d'origine dès que possible.

ARTICLE 11. TRANSMISSION ENTRE LES PARTIES

1. Les informations classifiées sont normalement transmises d'une Partie à l'autre par la voie diplomatique ou par d'autres voies convenues d'un commun accord entre les Parties, conformément aux lois et règlements internes de la Partie d'origine.

2. Lesdites transmissions répondent aux exigences suivantes :

a) la Partie d'origine doit s'assurer que la personne qui transmet les informations :

i. est un fonctionnaire ou un employé de la Partie d'origine ou de l'utilisateur d'origine ;

ii. est en possession d'une habilitation de sécurité personnelle d'un niveau au moins égal à celui des informations classifiées transmises ;

b) la personne qui fournit les informations classifiées doit être munie d'une lettre de l'autorité de sécurité compétente dans laquelle figurent :

i. l'autorisation pour la personne de transmettre des informations classifiées ;

ii. le point de contact de la Partie d'origine ;

iii. le point de contact de la Partie destinataire ;

c) la Partie d'origine consigne dans un registre les informations classifiées qui sont transférées et en remet une copie à la Partie destinataire sur demande. Les deux Parties transmettront les détails de ce registre à leur autorité de sécurité compétente ;

d) les informations classifiées sont correctement emballées et scellées conformément aux lois et règlements internes de la Partie d'origine ;

.

3. La transmission électronique d'informations classifiées doit se faire sous forme cryptée uniquement, à l'aide de méthodes et de dispositifs de cryptage mutuellement déterminés par les autorités de sécurité compétentes concernées.

ARTICLE 12. CONTRATS CLASSIFIÉS

1. Si l'autorité de sécurité compétente d'une Partie se propose de conclure, ou si un contractant relevant de sa juridiction se propose de conclure, un contrat classifié portant sur des informations classifiées de niveau CONFIDENCIAL/CONFIDENTIAL ou d'un niveau de classification supérieur avec un contractant relevant de la juridiction de l'autre Partie, elle est tenue d'obtenir en premier lieu la confirmation écrite de l'autorité de sécurité compétente de l'autre Partie, conformément à l'article 8 du présent Accord, selon laquelle le contractant s'est vu accorder l'habilitation de sécurité d'établissement ou l'habilitation de sécurité personnelle du niveau de classification approprié.

2. L'autorité de sécurité compétente qui a accordé une habilitation de sécurité d'établissement ou une habilitation de sécurité personnelle s'assure que les mesures de sûreté prises par le contractant soient conformes à sa législation et réglementation internes.

3. Aucune habilitation de sécurité d'établissement ou habilitation de sécurité personnelle n'est requise pour les contrats classifiés portant uniquement sur des informations classifiées de niveau DIFUSIÓN LIMITADA/RESTRICTED.

4. Tout contrat ou contrat de sous-traitance portant sur des informations classifiées comporte des dispositions relatives à la protection desdites informations. Lesdites dispositions donnent effet aux dispositions du présent Accord et à toute autre condition imposée par la Partie d'origine concernant l'utilisation d'informations classifiées. Seule la Partie d'origine peut modifier le niveau de classification des informations ou autoriser leur divulgation ultérieure.

5. L'autorité de sécurité compétente de la Partie d'origine transmet à l'autorité de sécurité compétente de la Partie destinataire une copie des dispositions en matière de sûreté d'un contrat.

ARTICLE 13. VISITES

1. Les visites effectuées par des ressortissants d'une Partie sur le site de l'autre Partie dans lequel des informations et du matériel classifiés sont conservés, sont autorisées sous réserve de l'accord préalable écrit de l'autorité de sécurité compétente de la Partie hôte. Les visites effectuées par des ressortissants d'États tiers dans des zones dans lesquelles des informations classifiées sont échangées entre les Parties ne sont autorisées que sur accord mutuel des Parties.

2. Les demandes de visite d'une Partie sont transmises par la voie diplomatique à l'autorité de sécurité compétente de la Partie hôte au moins trois semaines avant la date de la visite. Les demandes de visite contiennent les renseignements précisés à l'annexe A du présent Accord.

3. Chaque Partie peut demander une autorisation de visite pour une période maximale de douze mois. Si une visite en particulier est susceptible de ne pas être conclue dans le délai prévu par l'autorisation de visite, ou si un prolongement de la période prévue par l'autorisation de visite est nécessaire, la Partie requérante peut demander une nouvelle autorisation de visite sous réserve qu'elle soit effectuée au moins trois semaines avant l'expiration de l'autorisation en cours.

4. Tous les visiteurs doivent se conformer à la législation et réglementation internes de la Partie hôte concernant la protection des informations classifiées.

5. Les visites ne seront autorisées que si la personne est en possession d'une habilitation de sécurité personnelle appropriée et a un besoin d'en connaître.

ARTICLE 14. VISITES MULTIPLES

1. Pour tout projet, programme ou contrat classifié, les Parties peuvent établir des listes de personnels autorisés à effectuer des visites multiples conformément aux clauses et conditions convenues par les autorités de sécurité compétentes des Parties. Lesdites listes sont valables, dans un premier temps, pour une période de douze mois et, par accord entre les autorités de sécurité compétentes des Parties, la période de validité peut être prolongée pour de nouvelles périodes n'excédant pas douze mois au total.

2. Une fois ladite liste approuvée par l'autorité de sécurité compétente de la Partie hôte, les modalités des visites peuvent être convenues directement entre les établissements concernés.

ARTICLE 15. INCIDENTS DE SÉCURITÉ

1. En cas de suspicion ou de confirmation d'un incident de sécurité concernant des informations classifiées de l'autre Partie, la Partie concernée mène une enquête sur ledit incident et en informe immédiatement par écrit l'autorité de sécurité compétente de l'autre Partie.

2. La notification doit être suffisamment détaillée pour que la Partie d'origine puisse procéder à une évaluation complète des conséquences.

3. La Partie destinataire mène une enquête (avec, si nécessaire, l'aide de l'autre Partie) et prend toutes les mesures appropriées, conformément à sa législation et réglementation internes, afin d'en limiter les conséquences. La Partie destinataire informe la Partie d'origine des résultats de l'enquête et de toutes les mesures prises pour éviter qu'une telle situation ne se reproduise.

ARTICLE 16. FRAIS

En cas de frais, chaque Partie prend en charge les dépenses qu'elle a engagées dans le cadre des activités menées en vertu du présent Accord.

ARTICLE 17. RÈGLEMENT DES DIFFÉRENDS

Tout différend relatif à l'interprétation ou à l'application du présent Accord est réglé exclusivement par voie de consultations entre les Parties.

ARTICLE 18. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Aucune disposition du présent Accord ne réduit ou ne restreint tout droit de propriété intellectuelle (y compris les brevets et les droits d'auteur) associé aux informations classifiées transférées, auquel l'une des Parties, ses contractants ou toute tierce partie, peuvent prétendre.

ARTICLE 19. DISPOSITIONS FINALES

1. Chaque Partie notifie par écrit à l'autre Partie l'accomplissement de ses procédures internes nécessaires à l'entrée en vigueur du présent Accord, qui intervient le jour de la réception de la deuxième notification.

2. Le présent Accord peut être modifié à tout moment par consentement mutuel écrit des Parties. Les modifications entrent en vigueur selon la procédure établie au paragraphe 1 du présent article.

3. L'annexe fait partie intégrante du présent Accord.

4. Les autorités de sécurité compétentes peuvent conclure des accords de mise en œuvre du présent Accord.

5. Le présent Accord est conclu pour une période indéterminée. Chaque Partie peut dénoncer le présent Accord moyennant un préavis écrit de six mois adressé à l'autre Partie par la voie diplomatique.

6. Nonobstant la dénonciation du présent Accord, les obligations relatives à la protection des informations classifiées échangées dans le cadre de ce dernier sont maintenues.

7. En cas de dénonciation, tout contrat ou contrat de sous-traitance classifié continue d'être traité conformément aux dispositions du présent Accord, sauf accord contraire des Parties.

EN FOI DE QUOI, les soussignés, à ce dûment autorisés par leur gouvernement respectif, ont signé le présent Accord.

FAIT en double exemplaire à Madrid, le 16 décembre 2019, en langues espagnole et anglaise, les deux textes faisant également foi.

Pour le Royaume d'Espagne :
FERNANDO VALENZUELA MARZO
Secrétaire d'État aux relations extérieures

Pour la Nouvelle-Zélande :
FLETCHER TABUTEAU
Sous-Secrétaire d'État aux affaires étrangères

ANNEXE A

À L'ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LE GOUVERNEMENT DE LA NOUVELLE-ZÉLANDE RELATIF À LA PROTECTION D'INFORMATIONS CLASSIFIÉES DU 16 DÉCEMBRE 2019

DEMANDES DE VISITES

La demande de visite doit contenir les informations suivantes :

a) les noms et prénoms, la date et le lieu de naissance, la nationalité et le numéro de passeport (ou du document d'identité) du visiteur ;
b) le poste et les fonctions du visiteur, le nom de l'établissement de l'organisation qui l'emploie ;
c) le niveau et la date d'expiration de l'habilitation de sécurité personnelle du visiteur ;
d) la date proposée pour la visite et la durée prévue ;
e) l'objet de la visite et toute indication utile sur le sujet à traiter et les niveaux de classification des informations classifiées ;
f) le nom des établissements, installations et localités, l'objet de la visite ;
g) les noms et prénoms des personnes qui devraient recevoir le visiteur, si possible ;
h) la date, la signature et l'apposition du cachet officiel autorisé (de sécurité).