BOD

BOLETÍN OFICIAL DEL MINISTERIO DE DEFENSA

AÑO XXXIX • JUEVES, 6 DE JULIO DE 2023 • NÚMERO 131

SUMARIO

II. — RESOLUCIONES PARTICULARES CON RANGO DE REAL DECRETO

III. — PERSONAL

CVE: BOD-2023-s-131-461
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

SECRETARÍA DE ESTADO DE DEFENSA

DIRECCIÓN GENERAL DE PERSONAL

CUERPOS COMUNES DE LAS FUERZAS ARMADAS

EJÉRCITO DE TIERRA

CVE: BOD-2023-s-131-462
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

ARMADA

EJÉRCITO DEL AIRE Y DEL ESPACIO

GUARDIA CIVIL

MINISTERIO DEL INTERIOR

IV. — ENSEÑANZA MILITAR

MINISTERIO DE DEFENSA

CVE: BOD-2023-s-131-463
Verificable en https://sede.defensa.gob.es/acceda/bod

Página

V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Diseño y Maquetación:
Imprenta del Ministerio de Defensa

CVE: BOD-2023-s-131-464
Verificable en https://sede.defensa.gob.es/acceda/bod

II. — RESOLUCIONES PARTICULARES CON RANGO DE REAL DECRETO

MINISTERIO DE DEFENSA

Real Decreto 582/2023, de 4 de julio, por el que se promueve al empleo de General de Brigada del Cuerpo de Intendencia de la Armada al Coronel don Juan Pablo de Ory Arriaga.

A propuesta de la Ministra de Defensa, y previa deliberación del Consejo de Ministros en su reunión del día 4 de julio de 2023,

Vengo en promover al empleo de General de Brigada del Cuerpo de Intendencia de la Armada al Coronel don Juan Pablo de Ory Arriaga.

Dado en Madrid, el 4 de julio de 2023.

FELIPE R.

La Ministra de Defensa,
MARGARITA ROBLES FERNÁNDEZ

(B. 131-1)

(Del *BOE* número 159, de 5-7-2023.)

CVE: BOD-2023-131-18970
Verificable en https://sede.defensa.gob.es/acceda/bod

II. — RESOLUCIONES PARTICULARES CON RANGO DE REAL DECRETO

MINISTERIO DE DEFENSA

Real Decreto 593/2023, de 4 de julio, por el que se concede la Gran Cruz de la Real y Militar Orden de San Hermenegildo a los Oficiales Generales que se citan.

En consideración a lo solicitado por el personal que a continuación se relaciona y de conformidad con lo propuesto por la Asamblea de la Real y Militar Orden de San Hermenegildo,

Vengo en conceder la Gran Cruz de la referida Orden a los Oficiales Generales a continuación relacionados, con la antigüedad que para cada uno se señala.

Contralmirante del Cuerpo del Cuerpo General de la Armada, don Gonzalo Villar Rodríguez.
Antigüedad: 1 de agosto de 2022.

General de Brigada del Cuerpo General del Ejército de Tierra, don Alfonso Pardo de Santayana Galbis.
Antigüedad: 31 de enero de 2023.

General de Brigada del Cuerpo General del Ejército de Tierra, don Francisco Javier Lucas de Soto.
Antigüedad: 31 de enero de 2023.

General de Brigada del Cuerpo General del Ejército de Tierra, don Carlos Javier Frías Sánchez.
Antigüedad: 8 de febrero de 2023.

General de Brigada del Cuerpo General del Ejército de Tierra, don José Manuel Roy Calvo.
Antigüedad: 21 de febrero de 2023.

General de Brigada del Cuerpo General del Ejército de Tierra, don Jaime Vidal Mena Redondo.
Antigüedad: 21 de febrero de 2023.

General de Brigada del Cuerpo General del Ejército del Aire y del Espacio, don Jacobo Lecube Porrua.
Antigüedad: 28 de febrero de 2023.

General de Brigada Médico del Cuerpo Militar de Sanidad, don Alberto Hernández Abadía de Barbará.
Antigüedad: 2 de marzo de 2023.

General de Brigada Interventor del Cuerpo Militar de Intervención, don Miguel Ángel García Albarrán.
Antigüedad: 16 de marzo de 2023.

General de Brigada del Cuerpo General del Ejército de Tierra, don Juan Ignacio Reyes Madridejos.
Antigüedad: 17 de marzo de 2023.

CVE: BOD-2023-131-18971
Verificable en https://sede.defensa.gob.es/acceda/bod

General de Brigada del Cuerpo General del Ejército de Tierra, don Pablo Gómez Lera.

Antigüedad: 4 de abril de 2023.

General de Brigada del Cuerpo de Intendencia del Ejército de Tierra, don Alfonso Azores García.

Antigüedad: 4 de abril de 2023.

Dado en Madrid, el 4 de julio de 2023.

FELIPE R.

La Ministra de Defensa,
MARGARITA ROBLES FERNÁNDEZ

(B. 131-2)

(Del *BOE* número 159, de 5-7-2023.)

CVE: BOD-2023-131-18972
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

NORMALIZACIÓN

Resolución 200/11194/23

Cód. Informático: 2023015547.

Resolución del Jefe de Estado Mayor de la Defensa, por la que se implanta el Acuerdo de Normalización OTAN STANAG 3346.

En uso de las facultades que me confiere la Orden Ministerial 238/2002 de 14 de noviembre, por la que se aprueba el procedimiento para la implantación, ratificación, revisión y derogación de los Acuerdos de Normalización OTAN,

DISPONGO:

Primero. Se implanta en el ámbito del Ministerio de Defensa el STANAG 3346 AOS (Edición 9) «Señalamiento y balizamiento de obstáculos en campos de vuelo–AATMP-08, Edición B».

Segundo. El documento nacional de implantación será el propio STANAG 3346 AOS (Edición 9) –AATMP-08, Edición B.

Tercero. La fecha de implantación será la de su promulgación por la OTAN.

Madrid, 5 de junio de 2023.—El Almirante General Jefe de Estado Mayor de la Defensa, Teodoro Esteban López Calderón.

CVE: BOD-2023-131-19128
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

NORMALIZACIÓN

Resolución 200/11195/23

Cód. Informático: 2023016573.

Resolución del Jefe de Estado Mayor de la Defensa, por la que se implanta el Acuerdo de Normalización OTAN STANAG 2571.

En uso de las facultades que me confiere la Orden Ministerial 238/2002 de 14 de noviembre, por la que se aprueba el procedimiento para la implantación, ratificación, revisión y derogación de los Acuerdos de Normalización OTAN,

DISPONGO:

Primero. Se implanta en el ámbito del Ministerio de Defensa el STANAG 2571 MEDSTD (Edición 2) «Requisitos mínimos de las unidades de laboratorio en formaciones sanitarias de tratamiento en el teatro de operaciones–AMedP-8.5, Edición B».

Segundo. El documento nacional de implantación será el propio STANAG 2571 MEDSTD (Edición 2) –AMedP-8.5, Edición B.

Tercero. La fecha de implantación será la de su promulgación por la OTAN.

Madrid, 5 de junio de 2023.—El Almirante General Jefe de Estado Mayor de la Defensa, Teodoro Esteban López Calderón.

CVE: BOD-2023-131-19129
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

NORMALIZACIÓN

Resolución 200/11196/23

Cód. Informático: 2023016583.

Resolución del Jefe de Estado Mayor de la Defensa, por la que se implanta el Acuerdo de Normalización OTAN STANAG 2132.

En uso de las facultades que me confiere la Orden Ministerial 238/2002 de 14 de noviembre, por la que se aprueba el procedimiento para la implantación, ratificación, revisión y derogación de los Acuerdos de Normalización OTAN,

DISPONGO:

Primero. Se implanta en el ámbito del Ministerio de Defensa el STANAG 2132 MEDSTD (Edición 4) «Documentación relativa al tratamiento médico inicial y la evacuación– AMedP-8.1, Edición B».

Segundo. El documento nacional de implantación será el propio STANAG 2132 MEDSTD (Edición 4) –AMedP-8.1, Edición B.

Tercero. La fecha de implantación será la de su promulgación por la OTAN.

Madrid, 16 de febrero de 2023.—El Almirante General Jefe de Estado Mayor de la Defensa, Teodoro Esteban López Calderón.

CVE: BOD-2023-131-19130
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

TRANSFORMACIÓN DIGITAL

Cód. Informático: 2023016569.

Resolución 11197/2023, de 29 de junio, de la Secretaria de Estado de Defensa, por la que se aprueba la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa.

La Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (CIS/TIC) del Ministerio de Defensa (MDEF), que fue aprobada mediante la Orden DEF/2639/2015, de 3 de diciembre, pretende que las tecnologías en el ámbito CIS/TIC disponibles en cada momento, contribuyan a la consecución de los objetivos y capacidades del MDEF. Las capacidades y servicios CIS/TIC que satisfagan las necesidades de las Fuerzas Armadas en la toma de decisiones y la conducción de operaciones, serán prioritarias.

La Instrucción 14/2020, de 15 de abril, del Secretario de Estado de Defensa, por la que se aprueba la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital, en su actuación I.4, incluye la necesidad de investigar nuevas tecnologías y metodologías en el ámbito CIS/TIC y establecer su aplicación en el MDEF. La Inteligencia Artificial (IA) es uno de los principales catalizadores de la Transformación Digital y de la optimización de los recursos.

La Estrategia de Tecnología e Innovación para la Defensa (ETID 2020), aprobada mediante Resolución 300/01520/21, de 22 de enero, de la Secretaria de Estado de Defensa, incluye objetivos tecnológicos y líneas de I+D+i para el desarrollo de nuevas soluciones tecnológicas basadas en la IA dirigidas a su aplicación en el ámbito de la Defensa.

La Estrategia Nacional de Inteligencia Artificial (ENIA), publicada el 2 de diciembre de 2020, es un marco de referencia que orienta los planes sectoriales, estatales y estrategias regionales en esta materia en el periodo 2020-2025, en línea con las políticas desarrolladas por la Unión Europea, e impulsa la transformación de los diferentes sectores económicos mediante la cooperación público-privada.

La ENIA es uno de los ejes de la Agenda España Digital 2025, aprobada en julio de 2020, y uno de los componentes del Plan de Recuperación, Transformación y Resiliencia. Este documento identifica la IA como una de las tecnologías con mayor proyección e impacto en todas las áreas de actividad. También señala que la IA actúa como un catalizador de la investigación y la innovación, haciendo de la generación, almacenamiento y procesado masivo de datos (Big Data) un sector económico en sí mismo en el nuevo escenario digital y de desarrollo tecnológico. Finalmente, la IA tiene un fuerte impacto transformador en múltiples sectores de actividad, algunos sensibles y estratégicos, como la Sanidad, la Educación, o la Seguridad.

Asimismo, la Organización del Tratado del Atlántico Norte (OTAN) ha reconocido a la IA como una de las Tecnologías Emergentes y Disruptivas (EDT) que pueden potenciar las Capacidades de la Alianza y apoyar el desarrollo de sus misiones. En ese orden de cosas, en octubre de 2021 los Ministros de Defensa de la OTAN aprobaron la Estrategia de la Alianza en esta materia (NATO's Artificial Intelligence Strategy).

En el plano militar, la evolución del escenario estratégico está sustituyendo el concepto clásico de operaciones conjuntas por el de operaciones multidominio, en las cuales son imprescindibles unos sistemas de gestión de la información, mando y contro capaces, seguros e interoperables. En este sentido, los avances en las tecnologías de la información y de las aplicaciones militares de la IA, van a marcar la evolución del diseño y conducción de las operaciones.

Se prevé que la IA tenga una gran influencia en la forma en la que se configurará el campo de batalla. Las aplicaciones de la IA tendrán un impacto directo en todas las áreas que lo componen, destacando el de la gestión de la información, los procesos de obtención y explotación de inteligencia, la capacidad de disuasión, la toma de decisiones y el propio enfrentamiento. El empleo de la IA supondrá una revolución disruptiva, y es ya una herramienta transformadora más con capacidad de intervenir e influir decisivamente en muchos aspectos fundamentales de las operaciones.

CVE: BOD-2023-131-19131
Verificable en https://sede.defensa.gob.es/acceda/bod

Son muchos y de diversa índole los retos a los que se enfrenta el uso de la IA. Entre ellos, caben destacar aspectos éticos, tecnológicos, de disponibilidad de datos, de infraestructura, de sostenimiento de las soluciones, de protección de datos personales, etc. Por tanto, es necesario abordarlos si se quiere conseguir un uso ético y eficaz de la IA en el ámbito de la Defensa, lo que exigirá un esfuerzo coordinado de todos los organismos del Departamento.

Las personas que sirven en las Fuerzas Armadas son, y seguirán siendo, el activo más valioso del Departamento. Consecuentemente, en el MDEF se utilizarán datos e información, herramientas y aplicaciones habilitadas para la IA para mejorar el entendimiento y capacidades de las personas, no con el objetivo de reemplazarlas, sino de complementarlas y facilitar que aporten mayor valor a sus actividades, alineándose además con los principios éticos que sean de aplicación.

Los sistemas de IA que traten datos personales deberán cumplir los principios de licitud, lealtad y transparencia, minimización y exactitud de los datos, integridad y confidencialidad y responsabilidad proactiva, de acuerdo con las normas relativas a la protección de datos personales, recogidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Por lo expuesto, y para aprovechar el potencial de la IA, es preciso disponer de una estrategia para su desarrollo, implantación y uso en el ámbito del MDEF, coherente con las políticas ministeriales relacionadas, como son la Política CIS/TIC, Política de Seguridad de la Información y el proceso de Transformación Digital, la Política de I+D+i, y la Política de Armamento y Material.

La Estrategia que se presenta en esta Resolución servirá de referencia para que las iniciativas que se desarrollan en relación con la IA en los Ejércitos, la Armada y en el resto de ámbitos del MDEF, sean convergentes.

En su virtud, y en el ejercicio de la facultad que me confiere en artículo 4 del Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, y la disposición final primera de la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política CIS/TIC,

RESUELVO:

Artículo único. *Aprobación de la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa.*

Se aprueba la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición adicional única. *No incremento del gasto público.*

Las medidas incluidas en esta Resolución no supondrán incremento alguno de dotaciones, ni de retribuciones, ni de otros gastos de personal.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada cualquier disposición de igual o inferior rango que se opongan a lo establecido en esta Resolución.

Disposición final primera. *Facultades de aplicación.*

Se faculta al Director General del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) y al Director General de Armamento y Material (DGAM) para dictar, en el ámbito de sus respectivas competencias, las disposiciones oportunas para la aplicación de esta Resolución.

Disposición final segunda. *Entrada en vigor.*

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 29 de junio de 2023.—La Secretraria de Estado de Defensa, María Amparo Valcarce García.

CVE: BOD-2023-131-19132
Verificable en https://sede.defensa.gob.es/acceda/bod

ESTRATEGIA DE DESARROLLO, IMPLANTACIÓN Y USO DE LA INTELIGENCIA ARTIFICIAL EN EL MINISTERIO DE DEFENSA

CAPÍTULO I

Disposiciones Generales

Primero. *Finalidad*.

Esta Estrategia tiene por finalidad establecer la base para el desarrollo, implantación y uso de soluciones de Inteligencia Artificial (IA) en el Ministerio de Defensa (MDEF), que permitan incrementar la eficacia en las misiones y cometidos del Departamento.

Para ello, esta Estrategia establece y determina:

a) El contexto y la visión estratégica para el desarrollo, la implantación y el uso de la IA en el MDEF.

b) Los principios de desarrollo, implantación y uso responsable de la IA en el ámbito de la Defensa.

c) Las Líneas de Acción Estratégicas que deben guiar la adopción de la IA en el MDEF.

d) Las posibles áreas de aplicación y casos de usos actuales y futuros de esta tecnología para los cometidos del MDEF, dentro de los cuales tendrán prioridad los que tengan relación directa con el desempeño de las misiones y cometidos de las Fuerzas Armadas.

e) Una estructura de dirección y coordinación para el desarrollo, implantación y uso de aplicaciones basadas en IA en el MDEF.

f) Los mecanismos de coordinación entre todos los Centros o Unidades del MDEF con competencias en el desarrollo, implantación, y uso de soluciones basadas en IA.

Segundo. *Ámbito de Aplicación.*

La Estrategia de desarrollo, implantación y uso de la IA será de aplicación en todo el MDEF y sus Organismos Autónomos adscritos.

CAPÍTULO II

Visión general de la Inteligencia Artificial

Tercero. *Introducción y contexto.*

El MDEF pretende impulsar la adopción de esta tecnología y dotar a las Fuerzas Armadas de las capacidades que ofrece. El uso extensivo de la IA ha de facilitar al Departamento cumplir sus misiones y cometidos de manera eficaz y eficiente en un entorno cambiante.

En el ámbito militar, la IA está impactando de manera disruptiva en el imprevisible campo de batalla en el que las Fuerzas Armadas habrán de actuar para defender y salvaguardar los intereses nacionales, lo que significa un cambio de paradigma en el planeamiento y conducción de las operaciones militares.

La IA está modificando el entorno global de Seguridad y Defensa, ofreciendo una oportunidad sin precedentes para fortalecer la ventaja tecnológica del MDEF, pero también aumenta los riesgos y amenazas a los que se debe hacer frente. Esta tecnología afecta de modo transversal a todas las actividades militares desarrolladas por las Fuerzas Armadas en apoyo de sus tareas principales, defensa colectiva, gestión de crisis y seguridad cooperativa.

Se puede asumir como concepto general que la IA es la rama de la ciencia e ingeniería que permite diseñar y programar sistemas inteligentes capaces de resolver tareas en entornos inciertos y actividades hasta la fecha exclusivas de la inteligencia humana. Para ello se necesitan sensores que recopilen datos del entorno, medios para su almacenamiento, depuración, preparación y procesamiento de datos e identificación de patrones que recomienden acciones.

La IA engloba un conjunto de tecnologías que se incorporarán a los desarrollos futuros que se presten a ello, en beneficio de la Defensa y la Seguridad. Es necesario articular los medios y establecer las estructuras que permitan aprovechar el potencial de la IA para incidir positivamente en la actividad del Departamento, mejorando la eficacia y la agilidad de los procesos, sumándose al impulso de la Transformación Digital.

CVE: BOD-2023-131-19133
Verificable en https://sede.defensa.gob.es/acceda/bod

Para llevar a la práctica la visión estratégica del uso de la IA, es preciso identificar casos de uso apropiados que permitan aplicar las capacidades de esta tecnología en beneficio del desarrollo de las misiones y cometidos del Ministerio y, especialmente, de las Fuerzas Armadas, buscando el necesario alineamiento con las iniciativas que se estén llevando a cabo en el marco de las Organizaciones Internacionales de Seguridad y Defensa a las que España pertenece, en particular en el ámbito de la Unión Europea y de la Organización del Tratado del Atlántico Norte.

Con carácter general, y en línea con lo establecido en el eje estratégico del artículo 6.2. b) de la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, se priorizará la aplicación en el ámbito del Planeamiento Militar y en las capacidades militares derivadas.

Asimismo, se establecerá una estructura para involucrar a todos los ámbitos del MDEF en el desarrollo de soluciones y para aprovechar las capacidades disponibles.

Cuarto. *Definición de Inteligencia Artificial para el Ministerio de Defensa.*

El MDEF asumirá la definición de IA, redactada por la Comisión Europea y referenciada en la Estrategia Nacional de IA como sigue:

"Sistemas de software, y posiblemente también de hardware, diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas".

Quinto. *Visión estratégica de la Inteligencia Artificial.*

1. En el horizonte temporal próximo, la IA se integrará de manera extensiva en la actividad del MDEF, en general, y de las Fuerzas Armadas en particular. Su empleo se llevará a cabo siempre de forma identificable, estará dirigido a incrementar la eficacia en las misiones y cometidos del Departamento y será aplicable en todos los niveles orgánicos o de conducción de las operaciones. Su uso estará siempre de acuerdo con la legislación nacional e internacional, los principios de uso ético de la IA y dirigida a su área de aplicabilidad.

2. El MDEF explotará el uso militar potencial de la IA, a la vez que tomará las medidas necesarias para protegerse de su uso por parte de los posibles adversarios.

3. El MDEF promocionará la formación y el talento en IA, cuyo empleo estará sustentado sobre una sólida y robusta infraestructura de gestión y explotación del dato y promoverá una amplia, extensa y diversa colaboración con el resto de la Administración General del Estado, las Organizaciones Internacionales de Seguridad y Defensa de las que España forma parte, el sector privado, la Universidad y otros centros de investigación y conocimiento.

CAPÍTULO III

Pilares, principios y líneas de actuación estratégicas

Sexto. *Pilares del desarrollo, implantación y uso de la Inteligencia Artificial.*

Los pilares sobre los que se sustentará la aplicación de la IA en el MDEF serán los siguientes:

1. Gestión del dato.

a) La digitalización, la disponibilidad y el acceso a grandes volúmenes de datos provenientes de fuentes seguras y fiables son elementos imprescindibles para el desarrollo de la IA.

b) Dentro de la gestión del dato, el gobierno del dato constituye un elemento fundamental, a través del cual se establecen normas y procesos que velan por la calidad de los datos, su seguridad, trazabilidad y uso adecuado. Estas normas y procesos permitirán pasar de la artesanía de los modelos tradicionales a la explotación extensiva de la IA.

CVE: BOD-2023-131-19134
Verificable en https://sede.defensa.gob.es/acceda/bod

2. Infraestructuras para la IA.

El procesamiento de datos y la ejecución de algoritmos asociados al desarrollo, implantación y uso de la IA, requieren infraestructuras de alto rendimiento y capacidad, integradas en la Infraestructura Integral de Información para la Defensa (I3D). Aunque se puedan autorizar infraestructuras para la IA no integradas en la I3D para determinados casos, sus arquitecturas asegurarán siempre la interoperabilidad con la I3D, de forma que puedan emplear los servicios que provee esta infraestructura.

3. Investigación, desarrollo e innovación.

La aplicación de la IA en muchos ámbitos de interés para la Defensa plantea importantes retos éticos, tecnológicos y conceptuales, que necesitan ser abordados antes de hacer un uso operativo de las soluciones tecnológicas basadas en esta tecnología.

4. Formación, captación y retención del talento.

a) Para alcanzar el éxito en la explotación de la IA y, en su caso, contrarrestar su uso militar por parte de los posibles adversarios, es fundamental asegurar la preparación y capacitación en IA del personal del MDEF.

b) Para ello se deberán priorizar los procesos de incorporación, capacitación y retención de las personas que dispongan del talento necesario para posibilitar el uso de esta tecnología por el Departamento.

Séptimo. *Principios de desarrollo, implantación y uso responsable de la Inteligencia Artificial en la Defensa.*

Con el fin de lograr que la IA sea una tecnología fiable dirigida al cumplimiento de las misiones y cometidos del MDEF en general y de las Fuerzas Armadas en particular, se definen los siguientes principios que regirán su desarrollo, implantación y uso:

a) Legalidad: las aplicaciones de IA se desarrollarán y emplearán de acuerdo con el derecho nacional e internacional que sea de aplicación, incluida la Declaración Universal de Derechos Humanos y el Derecho Internacional Humanitario.

b) Responsabilidad humana y rendición de cuentas: cualquier desarrollo de IA, así como su utilización, deberá permitir una clara supervisión humana con el fin de garantizar la debida rendición de cuentas y la atribución de responsabilidades.

c) Inteligibilidad y trazabilidad: las aplicaciones de IA serán comprensibles y transparentes para el personal relevante, incluyendo el uso de metodologías, fuentes y procedimientos auditables.

d) Fiabilidad y transparencia: las aplicaciones de IA estarán dirigidas a casos de uso explícitos, bien definidos y acotados y se proporcionará información para fomentar una comprensión general de estas aplicaciones por todas las partes interesadas. La seguridad, la protección y la solidez de estas capacidades estarán sujetas a pruebas y garantías dentro de esos casos de uso a lo largo de todo su ciclo de vida.

e) Gobernabilidad: las aplicaciones de IA se desarrollarán y utilizarán de acuerdo con sus funciones previstas en el diseño, asegurando la capacidad de detectar y evitar consecuencias no intencionadas. Se habilitarán mecanismos de desconexión o desactivación cuando se reconozcan comportamientos no previstos o indeseados.

f) Mitigación del sesgo: se tomarán todas las medidas necesarias para minimizar errores y orientaciones subjetivas en el desarrollo y uso de aplicaciones de IA.

g) Privacidad: el desarrollo, la implantación y el uso de aplicaciones basadas en IA deben respetar la privacidad de las personas, desde el diseño y durante todo el ciclo de vida.

Octavo. *Resolución de conflictos éticos relacionados con la Inteligencia Artificial.*

1. La utilización de IA en sistemas de armas estará condicionada a la clara e inequívoca posibilidad de identificar a la persona responsable de su empleo directo y de la decisión de uso, de acuerdo con las directrices que establezca el MDEF en esta materia.

2. La resolución de conflictos éticos derivados del empleo de la IA será responsabilidad de las siguientes autoridades:

CVE: BOD-2023-131-19135
Verificable en https://sede.defensa.gob.es/acceda/bod

a) El Jefe de Estado Mayor de la Defensa, para las aplicaciones en el ámbito de las operaciones militares.

b) La persona titular de la Secretaría de Estado del Centro Nacional de Inteligencia, en el ámbito de sus competencias.

c) La persona titular de la Secretaría de Estado de Defensa, para el resto de aplicaciones.

3. Estas autoridades contarán con el apoyo del grupo de trabajo descrito en el capítulo V de esta Estrategia para analizar las cuestiones éticas relativas al desarrollo y empleo de la IA.

Noveno. *Líneas de Acción Estratégicas para el desarrollo, implantación y uso de Inteligencia Artificial en el Ministerio de Defensa.*

Teniendo en cuenta los principios y pilares sobre los que se sustenta el uso de la IA en el MDEF, se definen las siguientes Líneas de Acción Estratégicas:

1. Avanzar hacia una sólida infraestructura de información dentro de la I3D, de acuerdo con la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (CIS/TIC), para dar soporte a la IA.

En esta infraestructura se evaluará la posibilidad de hacer uso generalizado de la tecnología de nube aplicando el concepto de "nube primero". En la Estrategia de Explotación de la Nube en el Ministerio de Defensa, aprobada por la Resolución 307/08136/21, de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, se identifica como uno de sus principios este concepto de "nube primero". Se establecerá como modelo genérico de infraestructura de información que dé soporte a la IA en el MDEF con la finalidad de:

a) Potenciar el uso de la IA en las misiones estratégicas nacionales.

b) Priorizar el empleo de IA en todas las fases de las operaciones de las Fuerzas Armadas dentro del concepto de "nube de combate", que permita la distribución de datos y el intercambio de información dentro de un "espacio de batalla", donde cada usuario, plataforma o nodo autorizado contribuya y reciba información y puede explotarla en el transcurso de las operaciones militares. Este concepto se define igualmente en la Estrategia de Explotación de la Nube en el Ministerio de Defensa.

c) Extender las capacidades de la IA al "edge computing" en las operaciones de las Fuerzas Armadas. El concepto de "edge computing", traducido como "computación en el borde", hace referencia a la computación que tiene lugar en la ubicación más cercana a los datos, incluyendo las funciones que le permiten estar conectado, aunque sea de forma intermitente, al núcleo o a la nube.

Asimismo, la citada solidez se debe de extender a aquellas infraestructuras de información que, aplicando la tecnología de IA, no estén inicialmente integradas en la I3D, como pueden ser sistemas de armas, sistemas de control de plataforma, sensores, etc.

2. Potenciar las estructuras orgánicas responsables del desarrollo, implantación y uso de la IA.

Se reforzará la estructura de la Oficina del Director de Sistemas y Tecnologías de la Información y las Comunicaciones (Chief Information Officer -CIO) del MDEF y, en concreto, al Responsable Corporativo del Dato (Chief Data Officer -CDO), dada la relevancia de los datos como pilar para la IA, y al Responsable Corporativo de Tecnología (Chief Technology Officer-CTO). De forma complementaria y para asegurar la implantación global de las soluciones que se definan, se reforzarán las estructuras responsables de la gestión de datos en los diferentes ámbitos del MDEF.

Se reforzarán también las estructuras responsables de la seguridad de la información del MDEF, para responder a los retos que se derivan del uso de la IA.

Por último, se reforzará la estructura de I+D+i en el ámbito de la Dirección General de Armamento y Material, para poder abordar los retos tecnológicos asociados a la IA.

3. Potenciar las actividades de I+D+i en aplicaciones del ámbito de la Defensa que hagan uso de la IA, de acuerdo con los objetivos tecnológicos y líneas de I+D+i de la Estrategia de Tecnología e Innovación para la Defensa.

CVE: BOD-2023-131-19136
Verificable en https://sede.defensa.gob.es/acceda/bod

4. Potenciar y armonizar todas las áreas de la gestión del dato, para el entrenamiento de los modelos de IA y para garantizar la disponibilidad de datos de calidad para las aplicaciones asociadas del siguiente modo:

a) Promoviendo la generación, recopilación y etiquetado de datos en ámbitos en los que no existan o sean insuficientes.
b) Creando espacios de datos compartidos y repositorios accesibles.
c) Estableciendo mecanismos especiales para el tratamiento de datos clasificados o especialmente sensibles en el aspecto de la seguridad, aplicando la normativa vigente de seguridad de la información en función de la clasificación de ésta.
d) Promoviendo y asegurando la interoperabilidad de los datos entre las diferentes capacidades, dominios y comunidades de Interés.
e) Articulando mecanismos que favorezcan la reutilización de modelos y algoritmos ya desarrollados.
f) Manteniendo coherencia en la gestión del dato con la Administración General del Estado y con las Organizaciones Internacionales de Seguridad y Defensa.
g) Realizando el seguimiento y auditorías periódicas para comprobar el cumplimiento por parte de las soluciones de IA de la legislación y principios en vigor, a nivel nacional y de las Organizaciones Internacionales de Seguridad y Defensa.

5. Identificar desde fases tempranas del ciclo de Planeamiento de la Defensa, las funcionalidades que puedan requerir comportamientos inteligentes de los sistemas o la explotación avanzada de datos, de forma que sea posible adelantarse en la recopilación de datos y el desarrollo de las funcionalidades.

Se establecerán mecanismos que favorezcan la realimentación durante el ciclo de vida completo de las aplicaciones basadas en IA, desde su obtención hasta su sostenimiento.

6. Impulsar la formación en IA del personal del MDEF dentro el Plan Nacional de Competencias Digitales del siguiente modo:

a) Incluyendo en la enseñanza de formación y perfeccionamiento contenidos relativos a IA.
b) Incentivando las medidas necesarias para captar el talento en IA e incorporarlo al MDEF.

CAPÍTULO IV

Aplicabilidad de la Inteligencia Artificial en Seguridad y Defensa y áreas de aplicación y empleo prioritarias

Décimo. *Ámbito de aplicación de las tecnologías de Inteligencia Artificial.*

1. El MDEF comenzará el desarrollo de aplicaciones que incluyan IA de acuerdo con los principios de uso responsable fijados en el capítulo III.
2. La incorporación de IA se hará de manera progresiva, para generar un entorno de confianza en el Departamento, y siempre en el marco de las necesidades y prioridades establecidas en el Proceso de Planeamiento de la Defensa, regulada en la Orden Ministerial 60/2015, de 3 de diciembre, por la que se regula el proceso de Planeamiento de la Defensa. En todos los desarrollos y aplicaciones se tomará conciencia de que la IA apoya a la actividad, pero no la guía ni la dirige.

Undécimo. *Casos de uso iniciales de la Inteligencia Artificial.*

1. Teniendo en cuenta el amplio campo de aplicación de la IA, se establecen inicialmente los casos de uso en el MDEF que se describen en el apartado 2. Se basan e inspiran en los fijados en las Organizaciones Internacionales de Seguridad y Defensa y tienen en cuenta la disponibilidad de las infraestructuras de datos que permiten la adopción de IA.
2. Los ámbitos del MDEF determinarán y desarrollarán, en el marco del Proceso de Planeamiento de la Defensa, los campos de aplicación. En concreto, el Jefe de Estado

CVE: BOD-2023-131-19137
Verificable en https://sede.defensa.gob.es/acceda/bod

Mayor de la Defensa determinará los vinculados a las capacidades y operaciones militares siguientes:

a) Movilidad militar. Planeamiento y apoyo del transporte, estratégico, operacional y táctico.

b) Inteligencia. Interpretación de imágenes, análisis de datos y documental. Traducción automática de textos y del lenguaje hablado.

c) Guerra electrónica. Planeamiento y apoyo a las operaciones de Guerra Electrónica.

d) Autonomía en el comportamiento de sistemas no tripulados. Desarrollo de funciones autónomas no letales en sistemas no tripulados terrestres, navales y aeroespaciales.

e) Apoyo logístico y alistamiento operativo. Mantenimiento predictivo y sostenimiento. Esto incluye la implantación de bases logísticas inteligentes.

f) Conocimiento y vigilancia del entorno en los ámbitos terrestre, marítimo, aeroespacial, ciberespacial y cognitivo. Análisis masivo de datos, información y desinformación.

g) Ciberdefensa. Identificación y actuación frente a ciberamenazas. Incluye la prevención, predicción de ataques y simulación de su efecto en las redes y sistemas propios.

h) Apoyo a la toma de decisiones. Simulación y visualización de escenarios presentes y futuros para apoyar la adopción de decisiones en todos los niveles de conducción de las operaciones militares, estratégica, operacional y táctica.

i) Análisis geoespacial, meteorológico y oceanográfico. En apoyo al planeamiento, conducción y seguimiento de operaciones militares.

j) Gestión de la información, de la infraestructura y los servicios CIS/TIC. Asignación autónoma de recursos a servicios CIS/TIC en función de su carga de trabajo y previsión de actuaciones de mantenimiento, reposición y ampliación de los componentes de la infraestructura.

k) Gestión del talento y formación. Identificación de los candidatos más adecuados para los perfiles requeridos y apoyo a las actividades de enseñanza, instrucción y adiestramiento, incluyendo la simulación.

3. Estos casos de uso iniciales no impiden la incorporación de otros de interés para el MDEF.

CAPÍTULO V

Estructura de dirección, coordinación y apoyo

Decimosegundo. *Responsables del desarrollo, implantación y uso de Inteligencia Artificial en el Ministerio de Defensa.*

1. El responsable de la obtención, del desarrollo, implantación y uso de la IA en el MDEF será la persona titular de la Secretaría de Estado de Defensa. Para el ejercicio de esta responsabilidad se apoyará en la estructura de dirección, establecida en el dispositivo Decimotercero de esta Estrategia.

2. El Jefe de Estado Mayor de la Defensa será responsable de determinar, dentro del proceso integral de Planeamiento de la Defensa, las capacidades militares vinculadas a la IA, y el uso de las aplicaciones basadas en IA para el planeamiento y conducción de operaciones militares.

3. Las aplicaciones basadas en IA para la preparación y disponibilidad de la Fuerza, estarán desarrolladas conforme a las orientaciones y directrices del Jefe de Estado Mayor de la Defensa en su contribución a la Fuerza Conjunta y a su concepto de empleo, siendo los Jefes de Estado Mayor de los Ejércitos y de la Armada los responsables de su uso.

4. La responsabilidad del uso de aquellas aplicaciones basadas en IA para el desarrollo de las misiones y actividades del Centro Nacional de Inteligencia corresponderá a la persona titular de la Secretaría de Estado.

Decimotercero. *Estructura de dirección.*

1. La estructura de dirección estará copresidida por el Director General de Armamento y Material, como responsable de las políticas de investigación, desarrollo e innovación del

CVE: BOD-2023-131-19138
Verificable en https://sede.defensa.gob.es/acceda/bod

MDEF, y por el Director General del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), como responsable de la Políticas CIS/TIC, de Seguridad de la Información y Transformación Digital del MDEF.

2. Esta estructura es responsable del impulso y seguimiento de la implantación de esta Estrategia y de su alineamiento con la Política CIS/TIC, Política de Seguridad de la Información y proceso de Transformación Digital, Política de I+D+i y Política de Armamento y Material del MDEF.

3. Un representante del EMAD participará en las reuniones de esta estructura cuando se traten capacidades operativas.

Decimocuarto. *Estructura de coordinación y apoyo.*

1. Dependiendo de la estructura de dirección, se constituirá un Grupo de Trabajo Permanente de IA para el desarrollo, coordinación, seguimiento y control de esta Estrategia. Asesorará a las autoridades responsables del uso de la IA en el MDEF, en los aspectos éticos.

2. Este Grupo de Trabajo Permanente estará compuesto por los siguientes miembros:

a) Copresidencia compartida entre un representante de la Subdirección General de Planificación, Tecnología e Innovación y un representante del CESTIC, perteneciente a la Oficina del Chief Information Officer (CIO) del MDEF.

b) Vocales permanentes: representantes del Estado Mayor de la Defensa, Ejército de Tierra, Armada, Ejército del Aire y del Espacio, Unidad Militar de Emergencias, Dirección General de Armamento y Material, Centro Nacional de Inteligencia y CESTIC.

Se nombrará un único representante por cada uno de estos organismos.

c) Vocales no permanentes:

1.º Cuando se traten asuntos relativos a la formación, captación y retención del talento, participarán representantes de la Dirección General de Personal y de la Dirección General de Reclutamiento y Enseñanza Militar.

2.º Cuando sea necesario evaluar aspectos éticos, de protección de datos personales y jurídicos concernientes a las iniciativas y proyectos de IA, participarán representantes de la Asesoría Jurídica General de la Defensa y de la Oficina del Delegado de Protección de Datos Personales.

3.º Podrán designarse vocales no permanentes de organismos autónomos del MDEF con competencias en esta materia.

4.º El Grupo de Trabajo Permanente podrá convocar a representantes expertos de los ámbitos del MDEF para evaluar la aplicabilidad de la tecnología de IA en su actividad.

d) Participación externa: el Grupo de Trabajo Permanente podrá contar, cuando lo estime oportuno, con la participación de representantes de la Empresa, la Universidad, centros de investigación, otras instancias de la Administración General del Estado, o personalidades de reconocido prestigio relacionadas con esta materia.

e) Secretario: un oficial o funcionario designado por la presidencia.

3. El Grupo de Trabajo Permanente de IA se constituirá en un plazo no superior a seis meses desde la entrada en vigor de esta Estrategia y se reunirá con carácter periódico. Tendrá inicialmente los siguientes cometidos, que se desarrollarán de acuerdo con los términos de referencia que el propio Grupo establezca:

a) Asesorar a las Autoridades del MDEF y a la estructura de dirección, acerca de los aspectos éticos y jurídicos de las iniciativas y proyectos de IA.

b) Identificar las principales necesidades de soluciones tecnológicas basadas en IA del Departamento, incidiendo en aquéllas de carácter conjunto o común a varios ámbitos.

c) Realizar seguimiento de los casos de uso y proyectos en materia de IA para dar respuesta a necesidades identificadas, teniendo en cuenta los recursos disponibles y las posibilidades de coordinación con otros actores de la base tecnológica e industrial de la Defensa, promoviendo su ejecución o buscando alternativas de desarrollo en su caso.

d) Coordinar el intercambio de información de IA entre los organismos del Departamento involucrados en el desarrollo, implantación y uso de la IA.

CVE: BOD-2023-131-19139
Verificable en https://sede.defensa.gob.es/acceda/bod

e) Compartir y analizar los informes de diferentes fuentes de información que sean relevantes para el desarrollo, implantación y uso de la IA en el ámbito de la Defensa, así como sobre oportunidades de cooperación con otros organismos nacionales e internacionales relacionados con la IA.

f) Recopilar experiencias derivadas del uso de soluciones basadas en IA, que puedan realimentar los nuevos desarrollos.

g) Proponer la postura del MDEF en relación con la dimensión tecnológica de la IA, para su presentación en los foros y estructuras en los que participe el Departamento, tanto en el nivel nacional como internacional, y para la coordinación con otros actores implicados (universidades, asociaciones, centros de investigación y empresas).

h) Identificar fuentes de financiación adicionales a los Presupuestos Generales del Estado que puedan emplearse para proyectos de IA.

i) A propuesta de la Estructura de dirección, informar a la Comisión Permanente de la Comisión Ministerial de Administración Digital y, cuando se estime oportuno, elevar a la Comisión Ejecutiva CIS/TIC definida en la Orden Ministerial 2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, los resultados de las actividades, los riesgos y la problemática, así como de cualquier otro aspecto de relevancia en relación con la ejecución de los planes e iniciativas.

j) Impulsar y coordinar la actuación de una Red de Centros de Referencia de IA del Departamento con otros organismos públicos y privados con responsabilidad en esta materia.

En lo no previsto en esta Estrategia, el Grupo de Trabajo Permanente de IA ajustará su funcionamiento a las previsiones sobre órganos colegiados contenidas en la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Decimoquinto. *Red de Centros de Referencia de Inteligencia Artificial del Ministerio de Defensa.*

1. Se configurará una Red de Centros de Referencia para el seguimiento técnico de proyectos de IA, la compartición de resultados de estos proyectos, la mejora del conocimiento global en el MDEF y, en determinados casos, para el desarrollo de proyectos concretos y el establecimiento de entornos de experimentación.

2. Su actuación seguirá un modelo integrador, catalizador y dinamizador que facilite la sinergia entre ámbitos y proyectos, el apoyo mutuo, la optimización de recursos y el alineamiento con iniciativas nacionales, del sector público-privado e internacionales en materia de IA.

3. La Red de Centros de Referencia es la materialización de la "Comunidad de IA del MDEF", estará compuesto por las unidades, centros, estructuras u órganos con responsabilidad en IA que determinen los ámbitos del MDEF representados en el Grupo de Trabajo Permanente de IA. Éste convocará a los ámbitos para constituir formalmente la Red y elaborar sus términos de referencia.

4. Los componentes de la Red de Centros, aun manteniendo autonomía para desarrollar los proyectos que consideren oportunos dentro de su ámbito, pondrán en conocimiento del Grupo de Trabajo Permanente estas iniciativas o proyectos para que puedan identificarse aquellos potencialmente aprovechables por otros ámbitos, con objeto de hacer converger necesidades e incrementar la eficiencia en el empleo de recursos y la interoperabilidad.

CVE: BOD-2023-131-19140
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

HOMOLOGACIONES

Resolución 1A0/38273/2023, de 12 de junio, del Centro Criptológico Nacional, por la que se certifica la seguridad del producto «Huawei DOPRA SSP V300R005C00SPC123B200», solicitado por HUAWEI Technologies Co., Ltd.

Recibida en el Centro Criptológico Nacional la solicitud presentada por HUAWEI Technologies Co., Ltd., con domicilio social en F4 F Area Admnistration Building, Headquarters of Huawei Technologies Co., Ltd. Bantian, Longgang District, Shenzhen, 518129, República Popular de China, para la certificación de la seguridad del producto «Huawei DOPRA SSP V300R005C00SPC123B200», conforme al entorno de uso, garantías y limitaciones indicadas en la correspondiente Declaración de Seguridad: «Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023)».

Visto el correspondiente Informe Técnico de Evaluación de DEKRA Testing and Certification S.A.U., de código EXT-8470, que determina el cumplimiento del producto «Huawei DOPRA SSP V300R005C00SPC123B200», de las propiedades de seguridad indicadas en dicha Declaración de Seguridad, tras el análisis de su seguridad según indican las normas «Common Methodology for Information Technology Security Evaluation/Common Criteria for Information Technology Security Evaluation version 3.1 release 5».

Visto el correspondiente Informe de Certificación del Centro Criptológico Nacional, de código INF-4106, que determina el cumplimiento del producto «Huawei DOPRA SSP V300R005C00SPC123B200», de los requisitos para la certificación de su seguridad exigidos por el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, de 19 de septiembre.

De acuerdo con las facultades que me confiere la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, al amparo de lo dispuesto en el artículo 1 y artículo 2, párrafo 2, letra c, del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, al objeto de resolver la solicitud de certificación mencionada, dispongo:

Primero.

Certificar que la seguridad del producto «Huawei DOPRA SSP V300R005C00SPC123B200», cumple con lo especificado en la Declaración de Seguridad de referencia «Huawei DOPRA SSP V300R005C00SPC123B200 Security Target (version 1.3, 29/03/2023)», según exigen las garantías definidas en las normas «Common Methodology for Information Technology Security Evaluation/Common Criteria for Information Technology Security Evaluation version 3.1 release 5», para el nivel de garantía de evaluación EAL4 + ALC_FLR.1.

Segundo.

Esta certificación, su alcance y vigencia, y el uso de la condición de producto certificado, quedan sujetos a lo establecido en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

CVE: BOD-2023-131-19141
Verificable en https://sede.defensa.gob.es/acceda/bod

Tercero.

El Informe de Certificación y la Declaración de Seguridad citados se encuentran disponibles para su consulta en el Centro Criptológico Nacional.

Cuarto.

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 12 de junio de 2023.–La Secretaria de Estado Directora del Centro Criptológico Nacional, Esperanza Casteleiro Llamazares.

(B. 131-6)

(Del *BOE* número 158, de 4-7-2023.)

CVE: BOD-2023-131-19142
Verificable en https://sede.defensa.gob.es/acceda/bod

V. — OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

HOMOLOGACIONES

Resolución 1A0/38274/2023, de 19 de junio, del Centro Criptológico Nacional, por la que se certifica la seguridad del centro de producción «Sony Semiconductor Israel Secured Area», solicitado por Sony Semiconductor Israel Ltd.

Recibida en el Centro Criptológico Nacional la solicitud presentada por Sony Semiconductor Israel Ltd., con domicilio social en 6 HaHarash St., Hod HaSharon 4524079, Israel, para la certificación de la seguridad del centro de producción «Sony Semiconductor Israel Secured Area» ubicado en en 6 HaHarash St., Hod HaSharon, 4524079, Israel, conforme al entorno de uso, garantías y limitaciones indicadas en la correspondiente Declaración de Seguridad: «Sony Semiconductor Israel Site Security Target, v1.12, 28/10/2022».

Visto el correspondiente Informe Técnico de Evaluación de Applus Laboratories, de código EXT-8519, que determina el cumplimiento del centro de producción «Sony Semiconductor Israel Secured Area», de las propiedades de seguridad indicadas en dicha Declaración de Seguridad, tras el análisis de su seguridad según indican las normas «Common Methodology for Information Technology Security Evaluation/Common Criteria for Information Technology Security Evaluation version 3.1 release 5».

Visto el correspondiente Informe de Certificación del Centro Criptológico Nacional, de código INF-4115, que determina el cumplimiento del centro de producción «Sony Semiconductor Israel Secured Area», con los requisitos para la certificación de su seguridad exigidos por el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado por la Orden PRE/2740/2007, de 19 de septiembre.

De acuerdo con las facultades que me confiere la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, al amparo de lo dispuesto en el artículo 1 y artículo 2, párrafo 2, letra c, del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, al objeto de resolver la solicitud de certificación mencionada, dispongo:

Primero.

Certificar que la seguridad del centro de producción «Sony Semiconductor Israel Secured Area», cumple con lo especificado en la Declaración de Seguridad de referencia «Sony Semiconductor Israel Site Security Target, v1.12, 28/10/2022», según exigen las garantías definidas en las normas «Common Methodology for Information Technology Security Evaluation/Common Criteria for Information Technology Security Evaluation version 3.1 release 5», para los componentes de garantía de evaluación ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1 and AST_SSS.1.

Segundo.

Esta certificación, su alcance y vigencia, y el uso de la condición de centro de producción certificado, quedan sujetos a lo establecido en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

CVE: BOD-2023-131-19143
Verificable en https://sede.defensa.gob.es/acceda/bod

Tercero.

El Informe de Certificación y la Declaración de Seguridad citados se encuentran disponibles para su consulta en el Centro Criptológico Nacional.

Cuarto.

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 19 de junio de 2023.–La Secretaria de Estado Directora del Centro Criptológico Nacional, Esperanza Casteleiro Llamazares.

(B. 131-7)

(Del *BOE* número 158, de 4-7-2023.)

CVE: BOD-2023-131-19144
Verificable en https://sede.defensa.gob.es/acceda/bod