El Peruano
Firmado por: Editora Peru
Fecha: 24/11/2026 00:48

CONVENIOS INTERNACIONALES

Acuerdo entre el Gobierno de la República Tunecina y el Gobierno de la República del Perú sobre Supresión de Visas para Titulares de Pasaportes Diplomáticos, Especiales o de Servicio **135**
Entrada en vigor del «Acuerdo entre el Gobierno de la República Tunecina y el Gobierno de la República del Perú sobre Supresión de Visas para Titulares de Pasaportes Diplomáticos, Especiales o de Servicio» **135**

SEPARATA ESPECIAL

SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES

Res. SBS N° 02797-2026.- Aprueban los "Lineamientos sobre Buen Gobierno Corporativo para las Cajas Municipales de Ahorro y Crédito (CMAC)"

Diario Oficial El Peruano Electrónico (Ley N° 31649)

MUNICIPALIDAD DE ATE

Ordenanza N° 652-MDA.- Ordenanza que regula el proceso del Presupuesto Participativo Basado en Resultados en el distrito de Ate

MUNICIPALIDAD DE BREÑA

D.A. N° 011-026-MDB.- Prorrogan vigencia de beneficios tributarios establecidos en la Ordenanza N° 641-2026-MDB hasta el 30 de diciembre de 2026

MUNICIPALIDAD DE CHORRILLOS

Ordenanza N° 563-MDCH.- Ordenanza que regula la celebración de Matrimonio Civil Comunitario 2026

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Aprueban la Estrategia Nacional de Ciberseguridad 2026-2030

RESOLUCIÓN MINISTERIAL
N° 384-2026-PCM

Lima, 23 de noviembre de 2026

VISTOS: El Memorando N° D000828-2026-PCM-SGTD de la Secretaría de Gobierno y Transformación Digital; el Informe N° D000045-2026-PCM-SSTSD-ECV y el Informe N° D000018-2026-PCM-SSPRD-AZH, elaborados por la Subsecretaría de Tecnologías y Seguridad Digital y la Subsecretaría de Política y Regulación Digital, respectivamente; y,

CONSIDERANDO:

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos; así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, en ese sentido, el artículo 8 del citado Decreto Legislativo establece que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es el ente rector en materia de gobierno digital, la cual comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital, siendo responsable de dictar las normas, establecer los procedimientos en dicha materia, así como de garantizar su operación y correcto funcionamiento;

Que, el numeral 94.1 del artículo 94 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado mediante el Decreto Supremo N° 029-2021-PCM, dispone que el Marco de Seguridad Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), en su calidad de ente rector de la seguridad digital, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de fortalecer la confianza de los ciudadanos, entidades públicas y personas en general en el entorno digital;

Que, por su parte, el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional;

Que, conforme al artículo 4 del citado Decreto de Urgencia N° 007-2020, el Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital; y en concordancia con su artículo 5, la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es el ente rector en materia de Confianza Digital y el responsable de la articulación de cada uno de sus ámbitos: i) protección de datos personales y transparencia, ii) protección del consumidor y iii) seguridad digital;

Que, en esa misma línea, el literal h) del artículo 3 de la referida norma define a la ciberseguridad como la capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital; precisando expresamente que esta comprende la perspectiva técnica de la Seguridad Digital y constituye un ámbito del Marco de Seguridad Digital del país;

Que, el numeral 7.1 del artículo 7 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, crea el Centro Nacional de Seguridad Digital (CNSD) como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la

seguridad nacional, a fin de fortalecer la confianza digital; siendo responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos;

Que, en esa misma línea, el artículo 21 del Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, aprobado mediante el Decreto Supremo N° 157-2021-PCM, establece que las estrategias nacionales para la transformación digital son instrumentos activos, dinámicos y en constante actualización elaborados en el marco de la Política Nacional de Transformación Digital; las cuales comprenden, de manera no limitativa, a las estrategias nacionales sobre seguridad y confianza digital;

Que, la Política Nacional de Transformación Digital al 2030, aprobada mediante el Decreto Supremo N° 085-2023-PCM, establece como su Objetivo Prioritario 5 consolidar la seguridad y confianza digital en la sociedad. Para su efectivo cumplimiento, dispone la articulación de una estrategia nacional que provea la arquitectura y capacidades operativas necesarias para el monitoreo, identificación y respuesta ante incidentes de seguridad digital; garantice la protección y resiliencia de la infraestructura crítica; y fomente una cultura de ciberseguridad orientada a sensibilizar a la ciudadanía, fortaleciendo la confianza y asegurando el irrestricto respeto de los derechos humanos en el entorno digital;

Que, asimismo, en estricta concordancia con lo señalado, el Lineamiento 5.1 del Objetivo Prioritario 5 (OP5) de la citada Política Nacional de Transformación Digital exige asegurar el adecuado funcionamiento del Sistema Nacional de Transformación Digital mediante la elaboración y articulación de estrategias nacionales enfocadas en la seguridad y confianza digital, con el propósito ineludible de fortalecer las capacidades del país para mitigar riesgos cibernéticos y consolidar un entorno digital plenamente confiable para la sociedad;

Que, de conformidad con los artículos 82 y 83 del Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Resolución Ministerial N° 239-2026-PCM, la Secretaría de Gobierno y Transformación Digital (SGTD) es el órgano de línea con autoridad técnico-normativa a nivel nacional responsable de proponer, articular, implementar, supervisar y evaluar la Política Nacional de Transformación Digital y su estrategia, así como de formular y proponer estrategias y planes nacionales en las materias de su competencia; por lo que propone para su aprobación la Estrategia Nacional de Ciberseguridad 2026-2030 como instrumento orientador para la implementación de acciones en materia de ciberseguridad, en el marco de las competencias de la Presidencia del Consejo de Ministros;

Que, el Perú ha logrado avances significativos en la construcción de un sólido marco normativo e institucional en materia de ciberseguridad y confianza digital, impulsado por instrumentos como la Ley de Gobierno Digital y el Marco de Confianza Digital. Este ecosistema opera bajo la rectoría de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), y emplea al Centro Nacional de Seguridad Digital (CNSD) como la plataforma oficial encargada de gestionar, dirigir, articular y responder a los incidentes de seguridad digital a nivel nacional;

Que, no obstante, el principal desafío radica en una brecha estructural caracterizada por la insuficiente madurez técnico-operativa, tecnológica y de infraestructura del ecosistema nacional de ciberseguridad. Esta situación limita la implementación efectiva de los avances normativos alcanzados y compromete la capacidad del Estado para proteger los activos críticos nacionales, las actividades críticas y garantizar la continuidad de los servicios públicos esenciales frente a amenazas digitales;

Que, las buenas prácticas promovidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Unión Internacional de Telecomunicaciones (UIT), la Organización de los Estados Americanos (OEA) y las Naciones Unidas recomiendan que los Estados cuenten con estrategias nacionales de ciberseguridad como instrumentos de política pública para fortalecer la gobernanza, desarrollar capacidades institucionales, gestionar los riesgos cibernéticos, promover la cooperación y mejorar la resiliencia frente a las amenazas en el entorno digital;

Que, la Estrategia Nacional de Ciberseguridad 2026-2030 constituye un instrumento de carácter estratégico que orienta y articula la actuación de las entidades competentes para el fortalecimiento de la ciberseguridad a nivel nacional, conforme al marco normativo vigente, sin alterar la distribución de competencias, funciones y responsabilidades establecidas en el ordenamiento jurídico ni crear obligaciones distintas de las previstas en la legislación aplicable;

Que, por su naturaleza técnica, dinámica y altamente especializada, la Estrategia Nacional de Ciberseguridad se configura como el instrumento estratégico orientado a desarrollar el componente de ciberseguridad dentro del Marco de Seguridad Digital del Estado y del Marco de Confianza Digital, mediante la definición de prioridades nacionales, estándares técnicos y mecanismos de coordinación para la protección de las redes, sistemas, activos e infraestructura tecnológica frente a riesgos y amenazas en el entorno digital;

Que, en atención al problema público previamente identificado, corresponde aprobar la Estrategia Nacional de Ciberseguridad 2026 - 2030 como un instrumento de política pública que permita ordenar, articular y orientar las medidas y acciones destinadas a fortalecer la seguridad digital, gestionar los riesgos en el entorno digital y proteger las redes, sistemas y activos digitales del país, en concordancia con las competencias institucionales y el marco normativo vigente; que tiene como objetivos estratégicos: fortalecer las capacidades nacionales de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital en las entidades del ecosistema digital a nivel nacional; fortalecer la ciberseguridad de los activos críticos nacionales, las actividades críticas y los servicios públicos esenciales frente a amenazas de seguridad digital; desarrollar una cultura nacional de ciberseguridad y sólidas capacidades operativas en el talento humano del sector público y la ciudadanía; consolidar la cooperación internacional y el intercambio de información sobre amenazas de seguridad digital; fortalecer la gobernanza y el marco normativo en ciberseguridad en las entidades de la administración pública; y desarrollar capacidades nacionales de gestión de riesgos digitales e inteligencia en ciberseguridad en las entidades del Estado y sectores estratégicos;

Con el visado de la Secretaría de Gobierno y Transformación Digital, de la Oficina General de Planeamiento y Presupuesto y de la Oficina General de Asesoría Jurídica;

De conformidad con lo dispuesto en el numeral 8 del artículo 118 de la Constitución Política del Perú; la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 30096, Ley de Delitos Informáticos; la Ley N° 29733, Ley de Protección de Datos Personales; el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; y el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por la Resolución Ministerial N° 239-2026-PCM;

SE RESUELVE:

Artículo 1.- Aprobación de la Estrategia Nacional de Ciberseguridad 2026-2030

1.1. Aprobar la Estrategia Nacional de Ciberseguridad 2026-2030, la misma que forma parte integrante de la presente Resolución Ministerial.

1.2. La Estrategia Nacional de Ciberseguridad 2026-2030 constituye un instrumento de carácter estratégico, orientador y articulador de las acciones en materia de

ciberseguridad, cuya implementación se desarrolla conforme a las competencias de cada entidad y al marco normativo vigente.

Artículo 2.- Ámbito de aplicación

2.1 La presente Resolución Ministerial y la Estrategia Nacional de Ciberseguridad 2026-2030 se aplican a:

a) Las entidades de la Administración Pública establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2026-JUS, con excepción de las personas jurídicas señaladas en el numeral 8 del citado artículo.
b) Las empresas públicas de los gobiernos regionales y locales, y aquellas que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE).
c) Aquellos que se encuentren obligados al cumplimiento de obligaciones de acuerdo a la normativa vigente del marco de confianza digital y de activos críticos nacionales.

2.2 Las organizaciones del sector privado pueden tomar como referencia lo establecido en la presente Resolución Ministerial y en la Estrategia Nacional de Ciberseguridad 2026-2030 en cuanto les genere valor.

Artículo 3.- Conducción, articulación, supervisión y evaluación de la Estrategia Nacional de Ciberseguridad 2026-2030

3.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), en ejercicio de la rectoría nacional en materia de gobierno digital, seguridad digital y confianza digital, conduce, articula, supervisa y evalúa la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030.
3.2. Para el desarrollo de las acciones operativas vinculadas a la Estrategia Nacional de Ciberseguridad 2026-2030, la Secretaría de Gobierno y Transformación Digital (SGTD) actúa a través del Centro Nacional de Seguridad Digital (CNSD), el cual, de conformidad con el marco normativo vigente, gestiona, dirige, coordina y articula las acciones de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital.

Artículo 4.- Responsabilidades institucionales del Sector Público

4.1. Para la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 las entidades públicas articulan sus objetivos, acciones e iniciativas institucionales con los objetivos de la referida Estrategia, en el marco de sus funciones, competencias, capacidades institucionales y disponibilidad presupuestal, considerando los instrumentos del Sistema Nacional de Planeamiento Estratégico, según corresponda.
4.2. Los Comités de Gobierno y Transformación Digital promueven el seguimiento de la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 en sus respectivas entidades. Para dicho efecto, las entidades adoptan las medidas necesarias, de acuerdo con sus competencias, capacidades institucionales y disponibilidad presupuestal, a fin de:

a) Incorporar objetivos, indicadores y metas vinculados a la ciberseguridad en sus instrumentos de planeamiento institucional, cuando corresponda.
b) Incorporar iniciativas orientadas a la gestión de riesgos, mitigación de vulnerabilidades y fortalecimiento de los controles de ciberseguridad en sus instrumentos de gestión de gobierno digital.
c) Fortalecer las capacidades institucionales para la gestión de la seguridad digital y promover el adecuado ejercicio de las funciones del Oficial de Seguridad y Confianza Digital (OSCD) y la consolidación de los Equipos de Respuesta ante Incidentes de Seguridad Digital (CSIRT), conforme al marco normativo vigente.

Artículo 5.- Oficial de Seguridad y Confianza Digital

5.1. El Oficial de Seguridad y Confianza Digital (OSCD) desempeña un rol estratégico en la gestión de la seguridad digital de la entidad pública. En el marco de sus funciones, coordina, promueve y articula las acciones necesarias para fortalecer la gestión de la seguridad digital, incluyendo la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), sin perjuicio de las competencias que correspondan a las unidades orgánicas responsables de las tecnologías de la información y demás órganos involucrados, conforme a la estructura orgánica y al marco normativo vigente.
5.2. Para garantizar su independencia funcional respecto de las áreas de tecnologías de la información, el Oficial de Seguridad y Confianza Digital (OSCD) ejerce sus funciones con autonomía técnica y reporta a la máxima autoridad administrativa de la entidad y al Comité de Gobierno y Transformación Digital, del cual forma parte, conforme a la normativa vigente.

Artículo 6.- Responsabilidad por incumplimiento de entidades públicas

El incumplimiento de las obligaciones previstas en la normativa vigente relacionadas con la implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 genera las responsabilidades administrativas, civiles y penales que correspondan, de conformidad con el ordenamiento jurídico aplicable.

Artículo 7.- Seguimiento, Monitoreo y Evaluación

7.1. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), es la encargada de realizar el seguimiento, monitoreo y evaluación de la Estrategia Nacional de Ciberseguridad 2026-2030, en coordinación con el Centro Nacional de Seguridad Digital (CNSD) y las entidades responsables. Este proceso se ejecutará mediante:

a) Monitoreo semestral para verificar el avance de las acciones estratégicas.
b) Evaluación anual para determinar el cumplimiento de indicadores y metas.

7.2. Los resultados del seguimiento, monitoreo y evaluación constituyen insumos para la mejora continua de la Estrategia Nacional de Ciberseguridad 2026-2030 y sirven de base para la actualización de sus acciones, indicadores y metas, cuando corresponda, conforme a las competencias de la Secretaría de Gobierno y Transformación Digital (SGTD) y al marco normativo vigente.

Artículo 8.- Espacios de diálogo, articulación y participación

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital (SGTD), promueve mecanismos de diálogo, articulación y participación multisectorial para fortalecer la implementación, seguimiento, evaluación y mejora continua de la Estrategia Nacional de Ciberseguridad 2026-2030. Para tal efecto, puede convocar a las entidades públicas competentes, así como a representantes de la academia, el sector privado, la sociedad civil y organismos internacionales, conforme a sus competencias y al marco normativo vigente.

Artículo 9.- Financiamiento

9.1. La implementación de la Estrategia Nacional de Ciberseguridad 2026-2030 se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público y con cargo a los presupuestos institucionales autorizados.
9.2. Sin perjuicio de lo anterior, las entidades pueden gestionar recursos provenientes de la cooperación internacional no reembolsable y formular proyectos de inversión en el marco del Sistema Nacional de Programación Multianual y Gestión de Inversiones

(INVIERTE.PE) para el cierre de brechas en infraestructura de ciberseguridad.

Artículo 10.- Publicación
Disponer la publicación de la presente Resolución Ministerial y la Estrategia Nacional de Ciberseguridad 2026-2030, aprobada en el artículo 1, en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe), así como en la sede digital de la Presidencia del Consejo de Ministros (www.gob.pe/pcm), el mismo día de la publicación de la presente Resolución Ministerial en el Diario Oficial "El Peruano".

Artículo 11.- Vigencia
La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial El Peruano.

DISPOSCIONES COMPLEMENTARIAS FINALES

Primera.- Articulación interinstitucional en materia de seguridad digital
La Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros, a través del Centro Nacional de Seguridad Digital (CNSD), articula acciones con la Dirección Nacional de Inteligencia (DINI), el Comando Conjunto de las Fuerzas Armadas (CCFFAA), la Policía Nacional del Perú (PNP), la Autoridad Nacional de Protección de Datos Personales (ANPD), el Ministerio Público (MP), a través de sus órganos, y las demás entidades públicas competentes, con la finalidad de fortalecer las capacidades nacionales en materia de seguridad digital.
La articulación comprende el intercambio seguro de información, la cooperación técnica, el fortalecimiento de capacidades, la gestión de riesgos de seguridad digital, la adopción de medidas preventivas y de mitigación, la coordinación para la atención de incidentes de seguridad digital, la investigación y la persecución de delitos informáticos cuando corresponda, así como la promoción de buenas prácticas, conforme al marco normativo vigente en materia de gobierno digital, seguridad digital, confianza digital, protección de datos personales, delitos informáticos, defensa nacional e inteligencia.
La cooperación se desarrolla mediante mecanismos, protocolos y canales seguros de comunicación, en atención a la naturaleza y la clasificación de la información, así como a las obligaciones de confidencialidad, custodia y protección aplicables, con el fin de promover la complementariedad institucional y evitar la duplicidad de esfuerzos frente a riesgos, incidentes, delitos o amenazas que puedan comprometer la seguridad digital del Estado.

Segunda.- Adopción de estándares internacionales para la gestión de riesgos de seguridad digital en entornos industriales
Las entidades de la Administración Pública que administren, operen o sean responsables de gestionar sistemas de automatización y control industrial, y tecnología operativa (OT), adoptan e implementan normas técnicas y mejores prácticas globales en la gestión de riesgos en entornos industriales.
Para orientar y promover la seguridad de sistemas de automatización y control industrial, y tecnología operativa (OT) se puede considerar los siguientes estándares ISA/IEC 62443 (Seguridad de la información para sistemas de automatización y control industrial y la tecnología operativa), NIST SP 800-82 (Guía para la Seguridad de Tecnología Operativa), la norma ISO 22301 (Gestión de la continuidad del negocio), y otras de valor para el sector, industria o modelo de negocio. Estos estándares se implementan de manera complementaria a la normativa nacional vigente.

Regístrese, comuníquese y publíquese.

LUIS FERNANDO GALARRETA VELARDE
Presidente del Consejo de Ministros

2577750-1

COMERCIO EXTERIOR Y TURISMO

Designan miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones - MIGRACIONES en representación del Sector Comercio Exterior y Turismo

RESOLUCIÓN SUPREMA
N° 008-2026-MINCETUR

Lima, 22 de noviembre de 2026

CONSIDERANDO:

Que, mediante el artículo 1 del Decreto Legislativo Nº 1130 se crea la Superintendencia Nacional de Migraciones - MIGRACIONES, como un Organismo Técnico Especializado adscrito al Ministerio del Interior, con personería jurídica de derecho público interno, con autonomía administrativa, funcional y económica en el ejercicio de sus atribuciones;
Que, el artículo 8 del citado Decreto Legislativo establece que el Consejo Directivo es el órgano máximo de MIGRACIONES, responsable de establecer las políticas institucionales y la dirección de MIGRACIONES y se encuentra integrado por cuatro (4) miembros designados por Resolución Suprema. El Sector Interior propondrá dos (2) miembros, uno de los cuales será el Superintendente Nacional. Los Sectores Comercio Exterior y Turismo, y Relaciones Exteriores propondrán un (01) miembro cada uno, que los representarán en el Consejo Directivo;
Que, mediante Resolución Suprema N° 002-2026-MINCETUR se designa a la señora Ysabel Angeles Ramos Yañez, como miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
Que, la señora Ysabel Angeles Ramos Yañez ha formulado su renuncia como miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
Que, estando a lo propuesto por el Ministerio de Comercio Exterior y Turismo, se ha visto por conveniente aceptar la renuncia formulada y designar al nuevo miembro del Consejo Directivo de MIGRACIONES en representación del Sector Comercio Exterior y Turismo;
De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 31419, Ley que establece disposiciones para garantizar la idoneidad en el acceso y ejercicio de la función pública de funcionarios y directivos de libre designación y remoción; el Decreto Legislativo N° 1130, Decreto Legislativo que crea la Superintendencia Nacional de Migraciones - MIGRACIONES; la Ley N° 27790, Ley de Organización y Funciones del Ministerio de Comercio Exterior y Turismo; y, la Resolución Ministerial N° 216-2025-MINCETUR, que aprueba el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Comercio Exterior y Turismo;

SE RESUELVE:

Artículo 1.- Aceptar la renuncia formulada por la señora Ysabel Angeles Ramos Yañez, como miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones – MIGRACIONES en representación del Sector Comercio Exterior y Turismo, dándosele las gracias por los servicios prestados.
Artículo 2.- Designar a la señora Carmen Rocío Arévalo Martos, como miembro del Consejo Directivo de la Superintendencia Nacional de Migraciones – MIGRACIONES en representación del Sector Comercio Exterior y Turismo.