

REGISTRO OFICIAL[®]

ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

FUNCIÓN EJECUTIVA

ACUERDOS:

MINISTERIO DE DEFENSA NACIONAL:

374	Se designa al señor Crnl. EMC. Avilés León Hugo Fernando, como Director Ejecutivo del Instituto Geográfico Militar.....	2
-----	---	---

MINISTERIO DEL INTERIOR:

MDI-DMI-2026-0113-ACUERDO	Se reforma la conformación del Consejo Transitorio de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL)	5
---------------------------	--	---

RESOLUCIONES:

SERVICIO NACIONAL DE ADUANA DEL ECUADOR:

Se clasifican las siguientes mercancías:

SENAE-SGN-2026-0136-RE	VERSILAC, marca VERSILAC, fabricada por PROLIANT DAIRY INGREDIENTS.....	9
SENAE-SGN-2026-0137-RE	GOMITAS ENRIQUECIDAS CON VITAMINAS B1, B2, B6, B9, B12, A, D, Y E	14

FUNCIÓN DE TRANSPARENCIA Y CONTROL SOCIAL

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA:

SEPS-IGT-IGS-IGJ-INSESF-INR-INGINT-INSEPS-2026-0157	Se expide la Norma de control de seguridades en el uso de canales electrónicos para las entidades financieras del sector financiero popular y solidario	19
---	---	----



MINISTERIO
DE DEFENSA
NACIONAL

ACUERDO MINISTERIAL N° 374

Gian Carlo Loffredo Rendón
MINISTRO DE DEFENSA NACIONAL

CONSIDERANDO:

Que el artículo 154 de la Constitución de la República del Ecuador, dispone que las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, les corresponde: *“1. Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión”;*

Que el artículo 226 ibidem, determina: *“Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.”;*

Que el artículo 10 de la Ley Orgánica de la Defensa Nacional, establece como una de las atribuciones del ministro de Defensa Nacional, la siguiente: *“(...) g) Expedir las normas, acuerdos, reglamentos internos de gestión de aplicación general en las tres Ramas de las Fuerzas Armadas, así como los reglamentos internos de gestión de cada Fuerza; (...)”;*

Que el artículo 47 del Código Orgánico Administrativo, preceptúa: *“Representación legal de las administraciones públicas. La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley.”;*

Que el artículo 1 de la Ley de la Cartografía Nacional, establece: *“El Instituto Geográfico Militar (IGM) entidad de derecho público y personería jurídica, autonomía administrativa y patrimonio propio, orgánica y disciplinariamente subordinado a la Comandancia General del Ejército con sede en la ciudad de Quito, tendrá a su cargo y responsabilidad la planificación, organización, dirección, coordinación, ejecución, aprobación y control de las actividades encaminadas a la elaboración de la Cartografía Nacional y del Archivo de Datos Geográficos y Cartográficos del País”;*

Que el artículo 12 de la Ley ibidem, determina: *“El Director del Instituto Geográfico Militar, es el responsable de la marcha administrativa y disciplinaria del mismo (...)”;*

Que el artículo 26 del Reglamento a la Ley de Cartografía Nacional establece: *“El Director del Instituto Geográfico Militar será un Oficial General, graduado en la especialidad de Ingeniería, de preferencia en Ingeniería Geográfica, **designado por el Ministro de Defensa Nacional**, de acuerdo con la Ley de Personal de las Fuerzas Armadas (...)”;* (negritas fuera texto);

Que el artículo 27 del Reglamento ibidem, señala: *“El Subdirector del Instituto Geográfico Militar, será un Oficial en el grado de Coronel de Arma de Estado Mayor o Técnico, graduado en la especialidad de Ingeniería Geográfica, **designado por el Ministerio de Defensa Nacional** de acuerdo con la Ley de Personal de las Fuerzas Armadas (...)”;* (negritas fuera texto);

Que el artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, dispone: *“(...) Los Ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República, salvo los casos expresamente señalados en leyes especiales. Los Ministros de Estado, dentro de la esfera de su competencia, podrán delegar sus atribuciones y deberes al funcionario inferior jerárquico de sus respectivos Ministerios, (...) todo ello sin perjuicio de las funciones, atribuciones y obligaciones que de acuerdo con las leyes y reglamentos tenga el funcionario delegado (...)”;*

Que mediante Decreto Supremo N° 163, se creó el “Servicio Geográfico Militar”, publicado en el Registro Oficial No. 620 de 11 de abril de 1928;

Que a través del Decreto Ejecutivo N° 940, publicado en Registro Oficial Suplemento N° 581 de 22 de noviembre de 2011, el Instituto Geográfico Militar (IGM), se adscribe al Ministerio de Defensa Nacional;

Que el señor comandante general de la Fuerza Terrestre a través de la resolución de pases publicada en la Orden General de la Fuerza Terrestre N° 115 de 18 de junio de 2021, designa al señor CRNL EMC ACOSTA ÁLVAREZ PABLO ANÍBAL como director del Instituto Geográfico Militar;

Que la Coordinación General de Asesoría Jurídica del Ministerio de Defensa Nacional, mediante memorando N° MDN-JUR-2021-1145-ME de 05 de octubre de 2021, señala: *“(...) para la suscripción del Acuerdo Ministerial es necesario que se adjunte el perfil profesional del Oficial de conformidad con el artículo 26 del Reglamento a la Ley de Cartografía Nacional, en el caso de que no se cuente con un oficial General, deberá existir el respectivo informe de justificación en el que se establezca la imposibilidad de designar un Oficial con dicho rango (...)”;*

Que del informe N° FT-DGTH-UMP-MO-2026-043 de 15 de septiembre de 2026, el señor director general de Talento Humano de la Fuerza Terrestre, se desprende lo siguiente:

“(...) 3) CONCLUSIONES

- a. *El personal de señores oficiales Generales son designados a cumplir funciones directivas conforme a la disponibilidad, a la necesidad institucional y operacional.*
- b. *El señor CRNL EMC Hugo Fernando Avilés León cumple con los requerimientos establecidos para ser nombrado como Director del IGM.*
- c. *El señor CRNL EM Torres Garzón Augusto Marcelo cumple con los requerimientos establecidos para ser nombrado como Subdirector del IGM.*

4) RECOMENDACIONES

Me permito recomendar muy respetuosamente a usted mi General de Ejército que:

- a. *En vista del reducido número de señores oficiales Generales es necesario designar como Director del IGM un oficial con el grado de Coronel del arma de Ingeniería.*
- b. *Realizar los trámites administrativos a fin de realizar la designación de Director y Subdirector del IGM por parte del Ministerio de Defensa Nacional”, (negrillas de la fuente);*

Que mediante oficio N° FT-CGFT-DAP-SMP-2026-7959-O de 16 de septiembre de 2026, remite al señor subsecretario de Apoyo al Desarrollo Sector Defensa, señalando: *“En atención a Oficio Nro. MDN-SUD-2026-0758-OF del 07 de septiembre de 2026, mediante el presente me permito remitir a usted señor Subsecretario de Apoyo al Desarrollo Sector Defensa, el informe con sus respectivos anexos, para emisión del Acuerdo Ministerial de designación del Director y Subdirector del Instituto Geográfico Militar “;*

En ejercicio de las facultades previstas en el artículo 154, numeral 1) de la Constitución de la República del Ecuador, artículo 10, literal g) de la Ley Orgánica de la Defensa Nacional, y los artículos 26 y 27 del Reglamento a la Ley de Cartografía Nacional,

ACUERDA:

Art. 1.- Designar como director ejecutivo del Instituto Geográfico Militar, al señor CRNL EMC AVILES LEÓN HUGO FERNANDO, función que cumplirá desde el 16 de enero de 2026, conforme a lo dispuesto en la Orden General de la Fuerza Terrestre No. 238.

Art. 2.- Designar como subdirector del Instituto Geográfico Militar, al señor CRNL EM TORRES GARZÓN AUGUSTO MARCELO, función que cumplirá desde el 15 de julio de 2024, conforme a lo dispuesto en la Orden General de la Fuerza Terrestre N° 135.

Art. 3.- Formalizar, para efectos administrativos y de registro, las designaciones señaladas en los artículos 1 y 2 del presente Acuerdo Ministerial, respecto de los periodos indicados en los mismos, y reconocer el ejercicio de las funciones correspondientes durante dichos periodos.

Art. 4.- Remítase copia auténtica del presente Acuerdo Ministerial, al señor comandante general de la Fuerza Terrestre, para su conocimiento y trámite correspondiente.

Art. 5.- Las autoridades designadas, deberán cumplir con las disposiciones constitucionales, legales y reglamentarias; en todos los actos administrativos que ejecute o decida sobre la base de la presente designación, siendo responsables por la acción u omisión de este instrumento jurídico.

Art. 6.- El presente Acuerdo Ministerial, entrará en vigencia a partir de su suscripción sin perjuicio de su publicación en la Orden General Ministerial y en el Registro Oficial.

Publíquese y Comuníquese. -

Dado en el Ministerio de Defensa Nacional, en Quito D.M., **06-OCT-2026**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**GIAN CARLO LOFFREDO
RENDON**

Gian Carlo Loffredo Rendón
MINISTRO DE DEFENSA NACIONAL



**REPUBLICA DEL ECUADOR
MINISTERIO DE DEFENSA NACIONAL**



CERTIFICO. - Que el documento que en 03 (tres) páginas antecede, es fiel copia del documento firmado que consta en los Archivos Digitales de Ordenes Generales Ministeriales de la Dirección de Secretaría General de esta Cartera de Estado: **"Acuerdo Ministerial No. 374, del 06 de octubre de 2026; publicado en la Orden General Ministerial No. 156 de la misma fecha"**

Quito, D.M. 07 de octubre de 2026.



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**JOSE FRANCISCO
ZUNIGA ALBUJA**

**Sr. José Francisco Zúñiga Albuja
DIRECTOR DE SECRETARÍA GENERAL**



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**DARWIN VINICIO VACA
SAAVEDRA**

S.P. D. Vaca.

Base Legal: Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Defensa Nacional, con respecto a las atribuciones del director/a de Secretaría General en el Art. 9 numeral 3.2.6 de Gestión de Secretaría General literal d).
Instructivo para el almacenamiento y certificación de documentos institucionales firmados electrónicamente Art. 7 y 9.

ACUERDO Nro. MDI-DMI-2026-0113-ACUERDO

SR. JOHN REIMBERG OVIEDO
MINISTRO DEL INTERIOR

CONSIDERANDO:

Que, el artículo 82 de la Constitución de la República del Ecuador prescribe que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes;

Que, el artículo 154 numeral 1 de la Constitución de la República del Ecuador faculta a las ministras y ministros de Estado a ejercer la rectoría de las políticas públicas del área a su cargo, así como a expedir los acuerdos y resoluciones administrativas que se requieran para su gestión;

Que, el artículo 226 de la Constitución de la República del Ecuador dispone que las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán únicamente las competencias y facultades que les sean atribuidas en la Constitución y la ley, y coordinarán acciones para el cumplimiento de sus fines;

Que, el artículo 227 de la Constitución de la República del Ecuador establece que la administración pública constituye un servicio a la colectividad y se rige, entre otros, por los principios de eficacia, eficiencia, calidad, jerarquía, coordinación, planificación, transparencia y evaluación;

Que, el artículo 47 del Código Orgánico Administrativo establece que la máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetos a su competencia;

Que, el artículo 63 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público dispone que al ministerio rector de la seguridad ciudadana, protección interna y orden público le corresponde dirigir las políticas, planificación, regulación, gestión y control de la Policía Nacional;

Que, el artículo 64 numeral 4 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público determina como función del titular del ministerio rector de la seguridad ciudadana, protección interna y orden público ejercer la representación legal, judicial y extrajudicial de la Policía Nacional;

Que, el artículo 1 de la Ley de Creación de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), publicada en el Suplemento del Registro Oficial Nro. 495, de 08 de febrero de 2024, creó a dicha institución de educación superior y determinó como promotores de su creación al Ministerio del Interior y a la Policía Nacional;

Que, mediante Decreto Ejecutivo Nro. 381, de 30 de marzo de 2022, se creó el Ministerio del Interior como organismo de derecho público, con personalidad jurídica y autonomía técnica, administrativa, operativa y financiera, encargado de formular las políticas para seguridad ciudadana, protección interna y orden público;

Que, mediante Decreto Ejecutivo Nro. 541, de 21 de febrero de 2025, el Presidente de la República del Ecuador designó al señor John Reimberg Oviedo como Ministro del Interior;

Que, mediante Decreto Ejecutivo Nro. 11, de 27 de mayo de 2025, el Presidente de la República del Ecuador ratificó al señor John Reimberg Oviedo como Ministro del Interior;

Que, mediante Resolución RPC-SE-13-No.050-2024 dada a los veintitrés (23) días del mes de mayo de 2024, el Consejo de Educación Superior, emitió los lineamientos para el periodo de transición de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL) según lo previsto en su Ley de creación, la Ley Orgánica de Educación Superior (LOES) y la Constitución de la República del Ecuador;

Que, el artículo 6 de la Resolución ibídem, determinaba el periodo de funciones del Consejo Transitorio hasta que se constituya el Órgano Colegiado Superior y se cuente con autoridades definitivas, por un plazo no mayor a dos (2) años contados a partir de la conformación del Consejo Transitorio;

Que, mediante Acuerdo Nro. MDI-DMI-2024-0131-ACUERDO, de 25 de septiembre de 2024, se conformó el Consejo Transitorio de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL);

Que, mediante Acuerdo Nro. MDI-DMI-2025-0057-ACUERDO, de 30 de marzo de 2025, se rectificó el artículo 1 del Acuerdo Nro. MDI-DMI-2024-0131-ACUERDO, de 25 de septiembre de 2024;

Que, en el artículo 2 del Acuerdo Nro. MDI-DMI-2025-0057-ACUERDO, de 30 de marzo de 2025, consta la designación de los miembros del Consejo Transitorio de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL);

Que, con Resolución RPC-SO-38-No.674-2026 dada a los veintitrés (23) días del mes de septiembre de 2026, el Consejo de Educación Superior, resolvió Aprobar la propuesta de reforma a los *“Lineamientos para el periodo de transición de la Universidad de Seguridad Ciudadana y Ciencias Policiales”*, modificando en su contenido lo siguiente:

“Artículo 6.- Periodo de funciones.- El Consejo Transitorio funcionará hasta que se constituya el Órgano Colegiado Superior y se cuente con autoridades definitivas, por un plazo máximo de 5 años contados a partir de la conformación del Consejo Transitorio. Concluidas las funciones del Consejo Transitorio, este dejará de funcionar y, en consecuencia, las autoridades y representantes de los respectivos estamentos asumirán sus respectivas funciones, de lo cual se deberá informar al CES”.

Que, mediante Memorando Nro. PN-CGEN-POL-2026-14217-M, de 30 de septiembre de 2026, la Comandancia General de la Policía Nacional remitió al Ministerio del Interior el Informe Nro. PN-DNATH-DEIN-2026-1206-INF de 30 de septiembre de 2026, relacionado con la verificación del cumplimiento de requisitos aplicables a las designaciones de autoridades del Consejo Transitorio de la USECIPOL;

Que, el Informe Nro. PN-DNATH-DEIN-2026-1206-INF, de 30 de septiembre de 2026, concluye que *“El presente informe corresponde a una nueva verificación documental efectuada en atención al Memorando Nro. PN CGEN-POL-2026-14117-M, de fecha 29 de septiembre de 2026, aplicando a cada designación propuesta los requisitos previstos en los artículos 49, 51, 53 y 54 de la Ley Orgánica de Educación Superior, según corresponda, y las disposiciones pertinentes del Reglamento de Carrera y Escalafón del Personal Académico del Sistema de Educación Superior”*;

Que, el Informe Nro. PN-DNATH-DEIN-2026-1206-INF, de 30 de septiembre de 2026, en su numeral IV, determina que *“4.2 En el caso de la Dra. Gladis Margot Proaño Reyes, propuesta para Rectora, la documentación examinada contiene respaldo suficiente para verificar documentalmente los seis requisitos previstos en el artículo 49 de la LOES. 4.3 En el caso del Dr. Francisco Enrique Morán Peña, Ph.D., puesto a consideración para Vicerrector Académico, la documentación examinada contiene respaldo suficiente para verificar los requisitos previstos en el*

artículo 51 de la LOES, que remite a los mismos requisitos exigidos para ser Rector. 4.4 En el caso del Abg. Arturo Guillermo Clery Aguirre, Ph.D., puesto a consideración para Vicerrector Académico, la documentación examinada contiene respaldo suficiente para verificar los seis requisitos exigibles conforme al artículo 51, en concordancia con el artículo 49 de la LOES. Se acredita, entre otros aspectos, aproximadamente siete años de gestión educativa o experiencia equivalente en gestión y tres años, dos meses y veintiséis días como profesor universitario titular a tiempo completo al 29 de septiembre de 2026. 4.5 En el caso de la Dra. Vilma Noemí St. Omer Navarro, propuesta como Autoridad Académica, la documentación examinada contiene respaldo suficiente para verificar los cuatro requisitos previstos en el artículo 54 de la LOES. La certificación de la Universidad Católica de Santiago de Guayaquil, emitida el 30 de septiembre de 2026, acredita su desempeño como Docente Titular Principal desde el 28 de mayo de 1990 hasta el 31 de agosto de 2026, esto es, treinta y seis años, tres meses y tres días en dicha calidad, superando ampliamente el mínimo de cinco años exigido”.

Que, mediante Oficio Nro. MDI-VSI-SDP-2026-11616-OF, de 01 de octubre de 2026, se puso en conocimiento de la máxima autoridad del Ministerio del Interior Nro.

PN-DNATH-DEIN-2026-1206-INF, con la verificación de los requisitos de las autoridades académicas para integrar el Consejo Transitorio de la Universidad de Seguridad Ciudadana y Ciencias Policiales – USECIPOL;

Que, el Viceministro de Seguridad Ciudadana mediante sumilla contenida en la hoja de ruta del Oficio Nro. MDI-VSI-SDP-2026-11616-OF, dispone la elaboración del Acuerdo Ministerial correspondiente, estableciéndose la designación de la Dra. Gladis Margot Proaño Reyes como Rectora, del Abg. Arturo Guillermo Clery Aguirre, Ph.D., como Vicerrector Académico y de la Dra. Vilma Noemí St. Omer Navarro como Autoridad Académica; así como la permanencia en funciones de las autoridades académicas Ernesto Andrés Hermann Acosta y Pedro Colón Valdiviezo Salinas [Sic]; y la aceptación de la renuncia del Rector Diego José Romero Oseguera con efecto al 30 de septiembre de 2026. Sumilla que es clara y precisa al tenor del artículo 121 del Código Orgánico Administrativo; y,

En ejercicio de las facultades y atribuciones previstas en el artículo 154 numeral 1 de la Constitución de la República del Ecuador; el artículo 47 del Código Orgánico Administrativo; los artículos 63 y 64 numeral 4 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público; y, de conformidad con los artículos 3 y 4 de la Resolución Nro. RPC-SE-13-No.0050-2024 del Consejo de Educación Superior;

ACUERDA:

Artículo 1.- Aceptación de renuncia.- Aceptar la renuncia del Dr. Diego José Romero Oseguera, Ph.D., al cargo de Rector de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), con efecto al 30 de septiembre de 2026, conforme a la instrucción administrativa constante en el expediente.

Artículo 2.- Designaciones.- Reformar la conformación del Consejo Transitorio de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), respecto de las designaciones que se detallan a continuación:

1. Designar a la Dra. Gladis Margot Proaño Reyes para ejercer el cargo de **RECTORA** de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), al haber verificado el cumplimiento de los requisitos previstos en la Ley Orgánica de Educación Superior y demás normativa aplicable.
2. Designar al Abg. Arturo Guillermo Clery Aguirre, Ph.D., para ejercer el cargo de **VICERRECTOR ACADÉMICO** de la Universidad de Seguridad Ciudadana y Ciencias

Policiales (USECIPOL), al haber verificado el cumplimiento de los requisitos previstos en la Ley Orgánica de Educación Superior y demás normativa aplicable.

3. Designar a la Dra. Vilma Noemí St. Omer Navarro para ejercer el cargo de **AUTORIDAD ACADÉMICA** de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), al haber verificado el cumplimiento de los requisitos previstos en la Ley Orgánica de Educación Superior y demás normativa aplicable.

Artículo 3.- Autoridades que continúan en funciones.- Mantener en funciones al Mgs. Ernesto Andrés Hermann Acosta y al Dr. Pedro Colón Valdivieso Salinas, en calidad de **AUTORIDADES ACADÉMICAS** de la Universidad de Seguridad Ciudadana y Ciencias Policiales (USECIPOL), conforme a sus designaciones vigentes.

Artículo 4.- Régimen aplicable.- Las autoridades designadas mediante el presente Acuerdo deberán cumplir lo dispuesto en la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior, la Resolución Nro. RPC-SE-13-No.0050-2024 adoptada por el Pleno del Consejo de Educación Superior (CES) y su reforma dada con Resolución RPC-SO-38-No.674-2026, el Estatuto de la USECIPOL y demás normativa vigente y aplicable.

Artículo 5.- Ejecución y notificación.- De la ejecución y notificación del presente Acuerdo encárguese a la Comandancia General de la Policía Nacional, a través de las unidades administrativas correspondientes.

Artículo 6.- Permanencia de disposiciones previas.- Todo aquello que no esté previsto expresamente en la presente Acuerdo, se aplicará el contenido del Acuerdo Nro. MDI-DMI-2024-0131-ACUERDO del 25 de septiembre de 2024, reformado mediante el Acuerdo Nro. MDI-DMI-2025-0057-ACUERDO del 30 de marzo de 2025 y, siempre que no exista contraposición.

Artículo 7.- Vigencia.- El presente Acuerdo Ministerial entrará en vigencia a partir de su suscripción, sin perjuicio de su notificación, registro y publicación en el Registro Oficial; de lo cual se encargará la Dirección Administrativa del Ministerio del Interior.

COMUNÍQUESE Y PUBLÍQUESE.-

Dado en Quito, D.M., a los 09 día(s) del mes de Octubre de dos mil veintiséis.

Documento firmado electrónicamente

SR. JOHN REIMBERG OVIEDO
MINISTRO DEL INTERIOR



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOHN REIMBERG
OVIEDO

Resolución Nro. SENAE-SGN-2026-0136-RE**Guayaquil, 21 de septiembre de 2026****SERVICIO NACIONAL DE ADUANA DEL ECUADOR****RESOLUCIÓN ANTICIPADA EN MATERIA DE CLASIFICACIÓN ARANCELARIA****VISTOS:**

La solicitud de la ciudadana Soraya Natalia Almeida Boada, ingresada ante el Servicio Nacional de Aduana del Ecuador (SENAE) con formulario Nro. 136-2026-07-000272 de 02 de junio de 2026, quien en calidad de representante legal de la compañía BBJ SOLUCIONES ALIMENTICIAS S.A., con RUC No. 1792581893001, requiere que el Servicio Nacional de Aduana del Ecuador (SENAE) emita una Resolución Anticipada que establezca la clasificación arancelaria de la mercancía descrita como VERSILAC, fabricada por PROLIANT DAIRY INGREDIENTS, en presentación de sacos de 25 kg.

La competencia conferida al Director/a General del SENAE, establecida en el literal h) del artículo 216 del Libro V del Código Orgánico de la Producción, Comercio e Inversiones (COPCI).

Los Arts. 89, 90, 92 y 93 del Reglamento al Título de la Facilitación Aduanera para el Comercio del Libro V del Código Orgánico de la Producción, Comercio e Inversiones (COPCI), que reglamentan el procedimiento de resoluciones anticipadas conforme al Art. 141 del COPCI.

La Resolución No. SENAE-SENAE-2022-0011-RE, de 04 de febrero de 2022, de la Directora General del SENAE, publicada en el Segundo Suplemento del Registro Oficial # 635, de 08 de febrero de 2022, que expide el *“PROCEDIMIENTO QUE REGULA LA EMISIÓN DE RESOLUCIONES ANTICIPADAS”*.

La Resolución Nro. SENAE-SENAE-2022-0013-RE, de 08 de febrero de 2022, de la Directora General del SENAE, que delega al Subdirector General de Normativa Aduanera la facultad para emitir Resoluciones Anticipadas.

La declaración expresa del recurrente en el formulario adjunto a su solicitud de resolución anticipada, que, en cumplimiento a lo dispuesto en el Art. 16 de la Resolución No. SENAE-SENAE-2022-0011-RE, deja establecido que la solicitud: **a)** no ha sido presentada después de la transmisión de la declaración aduanera de la mercancía por la que está solicitando la resolución anticipada; **b)** la mercancía motivo de la solicitud de resolución anticipada no ha sido objeto de un reclamo administrativo, recurso de revisión, o acción judicial que esté pendiente de resolución o sentencia, o que haya sido resuelto previamente respecto a su clasificación arancelaria; **c)** no existe una investigación o proceso de control aduanero en curso por parte de la administración aduanera, respecto del solicitante, relacionado con la clasificación arancelaria de la mercancía por la que se solicita la resolución anticipada; **d)** desconoce de la existencia de resoluciones anticipadas de carácter general emitidas sobre mercancías idénticas a las que constan en la solicitud; **e)** la veracidad, exactitud, integridad y concordancia de la información y documentos proporcionados respecto de la mercancía objeto de resolución anticipada; y, **f)** no se ha solicitado la resolución anticipada después de transmitida la declaración aduanera y efectuado el levante de la mercancía, o, en caso de hacerse, con la finalidad de conocer la clasificación arancelaria de una mercancía idéntica a la declarada en esa ocasión, una vez obtenida la resolución anticipada, ésta no causará efecto sobre las declaraciones aduaneras transmitidas con anterioridad a su emisión, sino que registrará para las nuevas importaciones o exportaciones que se realicen sobre la mercancía idéntica.

El Arancel del Ecuador, adoptado mediante Resolución No. 002-2023 de El Pleno del Comité de Comercio Exterior (COMEX), en sesión de 02 de marzo de 2023 y en vigencia a partir de 01 de septiembre de 2023, publicado en el Segundo Suplemento del Registro Oficial No. 301 de 02 de mayo de 2023, que se fundamenta en la Nomenclatura Común de Designación y Codificación de Mercancías de los Países Miembros de la Comunidad Andina -NANDINA-, y ésta a su vez en el Convenio Internacional sobre el Sistema Armonizado de Designación y Codificación de Mercancías (Sistema Armonizado) del Consejo de Cooperación Aduanera,

actualmente Organización Mundial de Aduanas (OMA), en su Séptima Recomendación de Enmienda.

Las Reglas Generales para la Interpretación del Sistema Armonizado.

La Versión Única en Español de las Notas Explicativas del Sistema Armonizado (VUENESA).

El Oficio No. SENAE-SGN-2026-0778-OF de 30 de julio de 2026, mediante el cual se declara la admisibilidad de la solicitud a partir de su notificación, efectuada el 03 de agosto de 2026.

El informe técnico No. DNR-DTA-JCC-RVU-IF-2026-0345 de 13 de agosto de 2026, de la Dirección Nacional de Gestión de Riesgos y Técnica Aduanera.

CONSIDERANDO:

Que, de acuerdo a la información técnica del fabricante, la mercancía VERSILAC, es un suero permeado, también conocido como sólidos de la leche, obtenido mediante proceso de ultrafiltración, presentado en sacos de 25 kg.

Que, la mercancía tiene las siguientes características:

- Características físicas: Polvo color crema secado por aspersión, con un perfil de sabor suave. Es homogéneo, fluido y no se apelmaza.
- Consumo humano.
- Puede ser utilizado para reemplazar suero en polvo, lactosa, leche descremada en polvo, maltodextrina, dextrosa o sólidos de jarabe de maíz.
- Los sólidos de la leche son obtenidos al remover parte de la proteína, minerales y lactosa del suero. La separación se logra por ultrafiltración.
- Características/Beneficios: Aglomerado, altamente soluble. Carbohidrato natural. Aporte valioso de minerales. Potenciador de sabor natural (permite la reducción de sal, azúcar, y otros ingredientes o sabores más costosos).
- Aplicaciones: Mezclas para panificación / Productos de panificación. Mezclas para bebidas. Confeitería / Cubiertas / Rellenos. Productos lácteos / Dips / Helados. Alimentos preparados. Aderezos para ensaladas. Sazonadores para botanas. Sopas. Tabletas.
- Proceso productivo: Se fundamenta inicialmente en la ultrafiltración del suero dulce de leche (subproducto de la fabricación de queso), un proceso de separación que retiene la fracción proteica y genera como subproducto un permeado de suero líquido. Esta materia prima, que contiene aproximadamente un 25% de sólidos lácteos, es recibida e inspeccionada para luego ser pasteurizada a una temperatura mínima de 74.4 °C (166 °F) durante al menos 15 segundos, garantizando así su inocuidad microbiológica. Posteriormente, el líquido es concentrado mediante evaporación para reducir su humedad, se somete a una cristalización controlada de la lactosa y es secado por aspersión (spray drying), obteniendo un polvo con bajo contenido de humedad. Finalmente, el polvo obtenido pasa por un proceso de molienda para asegurar una granulometría uniforme.
- Su elaboración no contempla la adición de ingredientes que modifiquen su naturaleza láctea.

Composición		
Ingrediente	Típica	Especificación
Proteína (como tal)	2.9%	2.0% min.
Carbohidratos (Lactosa)	87.6%	80.0% min.
Grasa	0.1%	1.0% max.
Cenizas (Minerales)	7.9%	9.0% max.
Humedad	1.5%	3.5% max.
SPC (cfu/g)	<1,000	10,000 max.

Que, la Regla General 1 para la Interpretación del Sistema Armonizado dispone que: *"Los títulos de las Secciones, de los Capítulos o de los Subcapítulos sólo tienen un valor indicativo, ya que la clasificación está determinada legalmente por los textos de las partidas y de las Notas de Sección o de Capítulo y, si no son contrarias a los textos de dichas partidas y Notas, de acuerdo con las Reglas siguientes."*

Que, el texto de la partida arancelaria 04.04 detalla: *"Lactosuero, incluso concentrado o con adición de azúcar u otro edulcorante; productos constituidos por los componentes naturales de la leche, incluso con adición de azúcar u otro edulcorante, no expresados ni comprendidos en otra parte."*

Que, las notas explicativas de la partida arancelaria 04.04 describe en sus partes pertinentes:

"...Esta partida comprende el lactosuero (es decir, los componentes naturales de la leche que permanecen cuando se ha eliminado la materia grasa y la caseína) y el lactosuero modificado (véase la Nota 1 de subpartidas de este Capítulo). Estos productos se pueden presentar en estado líquido, pastoso o sólido (incluso congelado), incluidos los parcialmente deslactosados o desmineralizados y además concentrados (por ejemplo, en polvo) o conservados..."

Que, la mercancía al corresponder a un suero permeado, obtenido por un proceso de ultrafiltración del suero dulce de leche (subproducto de la fabricación de queso), que ha sido sometido a un proceso de ultrafiltración para extraer sus proteínas, y que según su proceso productivo no se adicionan ingredientes que modifiquen su naturaleza láctea, por lo que con base a los textos arancelarios expuestos y en concordancia con las características técnicas de la mercancía, en aplicación de la Primera Regla General para la Interpretación del Sistema Armonizado, a la mercancía motivo de consulta le corresponde clasificarse en la partida arancelaria 04.04.

Que, la Regla General 6 para la Interpretación del Sistema Armonizado, por su parte, señala que: *"La clasificación de mercancías en las subpartidas de una misma partida está determinada legalmente por los textos de estas subpartidas y de las Notas de subpartida así como, mutatis mutandis, por las Reglas anteriores, bien entendido que sólo pueden compararse subpartidas del mismo nivel. A efectos de esta Regla, también se aplican las Notas de Sección y de Capítulo, salvo disposición en contrario."*

Que, la mercancía al ser un lactosuero modificado, ya que es un subproducto resultante del procesamiento del lactosuero, al que se le ha extraído la proteína mediante ultrafiltración, se considera la nota de subpartida 1 del Capítulo 4 que detalla:

"...1. En la subpartida 0404.10, se entiende por lactosuero modificado el producto constituido por componentes del lactosuero, es decir, lactosuero del que se haya extraído, total o parcialmente, lactosa, proteínas o sales minerales, o al que se haya añadido componentes naturales del lactosuero, así como los productos obtenidos por mezcla de componentes naturales del lactosuero..."

Que, la nota complementaria NANDINA 1 del Capítulo 4 cita:

"...1. En la subpartida 0404.10.10 se entiende por lactosuero parcial o totalmente desmineralizado al lactosuero con un contenido en peso de: cenizas inferior o igual al 7 %; proteínas superior o igual a 10 % pero inferior o igual a 24 %; grasa superior o igual a 1 % pero inferior o igual a 4 %; lactosa inferior o igual a 82 % y humedad superior o igual a 1 % pero inferior o igual a 5 %..."

Que, la mercancía al corresponder a un suero permeado (lactosuero modificado), obtenido por un proceso de ultrafiltración del suero dulce de leche (subproducto de la fabricación de queso), que ha sido sometido a un proceso de ultrafiltración para extraer sus proteínas, y que no corresponde a la definición de lactosuero parcial o totalmente desmineralizado, por no cumplir en su composición lo detallado en la nota complementaria NANDINA 1 del Capítulo 4, su clasificación arancelaria procede en la subpartida "0404.10.90.00 - - Los demás", del Arancel del Ecuador, por aplicación de las Reglas Generales para la Interpretación del Sistema

Armonizado 1 y 6.

Que, por tanto, y

TENIENDO PRESENTE:

La competencia conferida al Director/a General del SENA E en el Art. 216 literal h) del COPCI; lo dispuesto en la Resolución No. SENA E-SENA E-2022-0011-RE; y, la delegación conferida por la Directora General del SENA E, de ese entonces, al suscrito Subdirector General de Normativa Aduanera mediante Resolución No. SENA E-SENA E-2022-0013-RE, dicto la siguiente:

RESOLUCIÓN ANTICIPADA:

Clasifíquese la mercancía denominada VERSILAC, marca VERSILAC, fabricada por PROLIANT DAIRY INGREDIENTS, presentada en sacos de 25 kg, que es un suero permeado, obtenido por un proceso de ultrafiltración del suero dulce de leche (subproducto de la fabricación de queso), que ha sido sometido a un proceso de ultrafiltración para extraer sus proteínas, conforme al análisis efectuado en los considerandos, en la subpartida del Arancel del Ecuador "0404.10.90.00 - - Los demás", por aplicación de las Reglas Generales para la Interpretación del Sistema Armonizado 1 y 6.

Se adjunta al presente dictamen de clasificación arancelaria el informe técnico Nro. DNR-DTA-JCC-RVU-IF-2026-0345 de 13 de agosto de 2026.

DISPOSICIONES FINALES:

Esta Resolución se mantendrá vigente mientras permanezcan los hechos o las circunstancias que la motivaron, las normas jurídicas en que se fundamentó, y la nomenclatura bajo la cual se emitió.

Encárguese a la Dirección de Secretaría General la notificación del contenido de la presente Resolución conforme a los datos registrados por el usuario que constan en la petición adjunta en documentos asociados del presente Quipux.

La presente Resolución entrará en vigencia a partir de su notificación al solicitante, sin perjuicio de su publicación en el Registro Oficial.

Encárguese a la Dirección de Secretaría General del Servicio Nacional de Aduana del Ecuador formalizar las diligencias necesarias para publicar la Resolución Anticipada en el Registro Oficial, la gaceta tributaria y en el portal web del Servicio Nacional de Aduana del Ecuador, respetando las condiciones de confidencialidad a las que se refiere el artículo 5 de la Resolución N° SENA E-SENA E-2022-0011-RE.

Documento firmado electrónicamente

Abg. David Andres Salazar Lopez
SUBDIRECTOR GENERAL DE NORMATIVA ADUANERA

Anexos:

- dnr-dta-jcc-rvu-if-2026-0345-signed-signed-signed-signed.pdf

Copia:

Señor Magíster
Luis Felipe Cedeño Puga
Director Nacional de Gestión de Riesgo y Técnica Aduanera

Señor Ingeniero
Luis Miguel Andino Montalvo

Director de Técnica Aduanera

Señora Magíster
Maria Veronica Ortiz Tanner
Jefe de Clasificación

Señor Licenciado
Ramon Enrique Vallejo Ugalde
Especialista en Técnica Aduanera

Señorita
María Gabriela Hinojosa Muñiz
Directora Secretaría General

revu/mvot/lmam/lfcv



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**DAVID ANDRES
SALAZAR LOPEZ**

Resolución Nro. SENAE-SGN-2026-0137-RE**Guayaquil, 21 de septiembre de 2026****SERVICIO NACIONAL DE ADUANA DEL ECUADOR****RESOLUCION ANTICIPADA EN MATERIA DE CLASIFICACIÓN ARANCELARIA****VISTOS:**

La solicitud del ciudadano Pierre Martel Tello, ingresada ante el Servicio Nacional de Aduana del Ecuador (SENAE) con formulario Nro. 136-2026-07-000271, de 02 de junio de 2026, quien en calidad de Representante Legal de la compañía SOTTCOR ECUADOR S.A.S., con RUC 0993394637001, solicita al Servicio Nacional de Aduana del Ecuador (SENAE) emitir una Resolución Anticipada en materia de Clasificación Arancelaria de la mercancía denominada comercialmente como "GOMITAS ENRIQUECIDAS CON VITAMINAS B1, B2, B6, B9, B12, A, D, Y E".

La documentación que consta en el Sistema Informático Ecuapass, mediante el cual se presenta información en respuesta de las observaciones realizadas por esta Subdirección General a través del Oficio No. SENAE-SGN-2026-0691-OF de 01 de julio de 2026, notificado el 02 de julio de 2026.

La documentación de soporte presentada por el solicitante dentro de su solicitud de resolución anticipada en materia de clasificación arancelaria, consistente en: ficha técnica y demás documentación técnica emitida por el fabricante: SOTTCOR LABS S.A.C PERU; e imágenes de la mercancía objeto de la presente solicitud.

El requerimiento del solicitante de tratar con carácter confidencial la información concerniente a la solicitud de resolución anticipada.

La competencia conferida al Director/a General del SENAE, establecida en el literal h) del artículo 216 del Libro V del Código Orgánico de la Producción, Comercio e Inversiones (COPCI).

La Resolución No. SENAE-SENAE-2022-0011-RE, de 04 de febrero de 2022, de la Directora General del SENAE, publicada en el Segundo suplemento No. 635 del Registro Oficial, de 08 de febrero de 2022, que expide el "**PROCEDIMIENTO QUE REGULA LA EMISIÓN DE RESOLUCIONES ANTICIPADAS**".

La Resolución No. SENAE-SENAE-2022-0013-RE, de 08 de febrero de 2022, de la Directora General del SENAE, que delega al Subdirector General de Normativa Aduanera la facultad para emitir resoluciones anticipadas.

El Arancel del Ecuador, adoptado el 1ro de septiembre de 2017 mediante Resolución 020-2017 del Comité de Comercio Exterior (COMEX), que se fundamenta en la Nomenclatura Común de Designación y Codificación de Mercancías de los Países Miembros de la Comunidad Andina -NANDINA-, y ésta a su vez en el Convenio Internacional sobre el Sistema Armonizado de Designación y Codificación de Mercancías (Sistema Armonizado) del Consejo de Cooperación Aduanera, actualmente Organización Mundial de Aduanas (OMA), en su Sexta Recomendación de Enmienda.

Las Reglas Generales para la Interpretación del Sistema Armonizado.

La Versión Única en Español de las Notas Explicativas del Sistema Armonizado (VUENESA).

El Oficio No. SENAE-SGN-2026-0785-OF, de 31 de julio de 2026, mediante el cual se declara la admisibilidad de la solicitud a partir de su notificación, efectuada el 31 de julio de 2026.

El informe técnico No. **DNR-DTA-JCC-FAFV-IF-2026-0376**, de 11 de septiembre de 2026, y su documento anexo (lista de equipos) de la Dirección Nacional de Gestión de Riesgos y Técnica Aduanera.

CONSIDERANDO:

Que, de acuerdo a lo que consta en la documentación técnica presentada por el requirente, la mercancía objeto de consulta denominada comercialmente “GOMITAS ENRIQUECIDAS CON VITAMINAS B1, B2, B6, B9, B12, A, D, Y E”, presentada en envases PET de 150 gomitas, corresponde a una preparación alimenticia complementaria para adultos en forma de caramelos blandos dulces. Su formulación está constituida por gelatina, glucosa, miel de abeja, azúcar, almidón, pectina, agua, panela, sabor a tutti frutti, glucósidos de esteviol y ácido cítrico, que cumplen funciones de excipientes; vitaminas A, B1, B2, B6, B9, B12, D y E, que actúan como ingredientes activos; y sorbato de potasio, utilizado como conservante. Se encuentra destinada al consumo directo por vía oral, con una dosis recomendada de 1 gomita diaria para niños de 2 a 3 años, 2 gomitas diarias para niños de 3 a 4 años y 4 gomitas diarias para niños de 9 a 15 años; y según se indica en la ficha técnica es un producto que tiene la finalidad de complementar la dieta habitual, proporcionando nutrientes que participan en procesos metabólicos, manteniendo las estructuras corporales y funciones fisiológicas normales de niños y jóvenes de las edades antes mencionadas.

Que, la mercancía en estudio cuenta con las siguientes características:

- Color: naranja
- Sabor y olor: característico

Que, el solicitante ha requerido que la información concerniente a su solicitud de resolución anticipada sea tratada con carácter confidencial, por consiguiente, al tenor de lo establecido en el artículo 5 de la Resolución Nro. SENAE-SENAE-2022-0011-RE se limita a tal efecto en esta resolución la publicación de información relativa que consta en la etiqueta de la mercancía objeto de consulta.

Que, la Regla General 1 para la Interpretación de la Nomenclatura del Sistema Armonizado dispone que: *"Los títulos de las Secciones, de los Capítulos o de los Subcapítulos sólo tienen un valor indicativo, ya que la clasificación está determinada legalmente por los textos de las partidas y de las Notas de Sección o de Capítulo y, si no son contrarias a los textos de dichas partidas y Notas, de acuerdo con las Reglas siguientes."*

Que, el capítulo 17 de la nomenclatura del Sistema Armonizado comprende los “Azúcares y artículos de confitería” y el capítulo 21 de la nomenclatura del Sistema Armonizado comprende los “Preparaciones alimenticias diversas”.

Que, la partida 17.04 de la nomenclatura del Sistema Armonizado comprende los “Artículos de confitería sin cacao (incluido el chocolate blanco).” y la partida 21.06 de la nomenclatura del Sistema Armonizado comprende las “Preparaciones alimenticias no expresadas ni comprendidas en otra parte.”.

Que, las notas explicativas de la partida 17.04, establecen: *“Esta partida comprende la mayor parte de las preparaciones alimenticias azucaradas sólidas o semisólidas dispuestas ya, en general, para su consumo inmediato y comúnmente designadas con el nombre de artículos de confitería o dulcería...”*.

Que, las notas explicativas de la partida 21.06, establecen: *“Con la condición de no estar clasificadas en otras partidas de la Nomenclatura, esta partida comprende:*

A) Las preparaciones que se utilizan tal como se presentan o previo tratamiento (cocción, disolución o ebullición en agua o leche, etc.) en la alimentación humana.

(...)

Están comprendidos en esta partida, entre otros:

(...)

16) *Las preparaciones frecuentemente conocidas con el nombre de complementos alimenticios a base de extractos de plantas, concentrados de frutas u otros frutos, miel, fructosa, etc., con adición de vitaminas y, a veces, cantidades muy pequeñas de compuestos de hierro. Estas preparaciones suelen presentarse en envases indicando que se destinan a mantener el organismo en buen estado de salud. Se excluyen de esta partida las preparaciones análogas destinadas a prevenir o tratar enfermedades o afecciones (partida 30.03 ó 30.04)...*" (el subrayado no es parte del texto original).

Que, al tratarse de GOMITAS ENRIQUECIDAS CON VITAMINAS B1, B2, B6, B9, B12, A, D, Y E, mercancía que según se indica en la ficha técnica presentada, es una preparación alimenticia complementaria para niños y jóvenes en forma de caramelos blandos dulces, que además de los componentes empleados como vehículo de administración, está formulada con ingredientes funcionales (vitaminas B1, B2, B6, B9, B12, A, D y E) específicamente dosificados por porción. Asimismo, la documentación técnica atribuye a dichos ingredientes beneficios relacionados con la complementación de la dieta habitual, proporcionando nutrientes que participan en proceso metabólicos, mantenimiento de estructuras corporales y funciones fisiológicas normales. Adicionalmente, tanto la etiqueta como la ficha técnica, establecen una dosis recomendada, evidenciando que la mercancía se encuentra destinada a complementar la alimentación humana. En virtud de sus características objetivas, composición, forma de presentación y uso previsto, se considera que la mercancía no se encuentra concebida para su consumo como artículo de confitería o dulcería, por lo que se descarta su clasificación arancelaria en la partida 17.04. En consecuencia, considerando que es una preparación alimenticia destinada al consumo humano que no se encuentra expresada ni comprendida en otra parte de la nomenclatura, ésta debe clasificarse en la partida 21.06, en aplicación de la Regla General 1 para la Interpretación del Sistema Armonizado.

Que, la Regla General 6 para la Interpretación de la Nomenclatura del Sistema Armonizado, por su parte, señala que: *"la clasificación de mercancías en las subpartidas de una misma partida está determinada legalmente por los textos de estas subpartidas y de las Notas de subpartida así como, mutatis mutandis, por las Reglas anteriores, bien entendido que sólo pueden compararse subpartidas del mismo nivel. A efectos de esta Regla, también se aplican las Notas de Sección y de Capítulo, salvo disposición en contrario."*

Que, la subpartida nacional 2106.90.74.00 del Arancel del Ecuador, según Resolución No. 002-2023 del COMEX, comprende a preparaciones alimenticias *"- - - Que contengan como ingrediente principal una o más vitaminas"* y que no se encuentran expresadas o comprendidas en otra de la nomenclatura.

Que, la mercancía en estudio es una preparación alimenticia para consumo humano, presentada en forma de caramelos blandos dulces, concebida como complemento alimenticio para niños y jóvenes al establecer una dosis de consumo recomendada y atribuirse a sus componentes beneficios relacionados con la complementación de la dieta habitual, proporcionando nutrientes que participan en proceso metabólicos, mantenimiento de estructuras corporales y funciones fisiológicas normales; función que se sustenta principalmente en la presencia de vitaminas B1, B2, B6, B9, B12, A, D y E, como ingredientes activos y; por lo tanto, se debe clasificar en la subpartida **"2106.90.74.00 - - - Que contengan como ingrediente principal una o más vitaminas"** del Arancel del Ecuador, por aplicación de las Reglas Generales para la Interpretación del Sistema Armonizado **1** (texto de la partida 21.06) y **6**.

Que, por tanto, y

TENIENDO PRESENTE:

La competencia conferida al Director/a General del SENA en el Art. 216 literal h) del COPCI; lo dispuesto en la Resolución No. SENA-SENAE-2022-0011-RE; y, la delegación conferida por la Directora General del SENA, Sra. Carola Soledad Ríos Michaud, al suscrito Subdirector General de Normativa Aduanera mediante Resolución No. SENA-SENAE-2022-0013-RE, dicto la siguiente:

RESOLUCIÓN ANTICIPADA:

Clasifíquese la mercancía denominada "**GOMITAS ENRIQUECIDAS CON VITAMINAS B1, B2, B6, B9, B12, A, D, Y E**", conforme al análisis efectuado en los considerandos, en la subpartida del Arancel del Ecuador "**2106.90.74.00 - - - Que contengan como ingrediente principal una o más vitaminas**", al tratarse de una preparación alimenticia para consumo humano, presentada en forma de caramelos blandos dulces, concebida como complemento alimenticio para niños y jóvenes al establecer una dosis de consumo recomendada y atribuirse a sus componentes beneficios relacionados con la complementación de la dieta habitual, proporcionando nutrientes que participan en proceso metabólicos, mantenimiento de estructuras corporales y funciones fisiológicas normales; función que se sustenta principalmente en la presencia de vitaminas B1, B2, B6, B9, B12, A, D y E, como ingredientes activos; por aplicación de las Reglas Generales para la Interpretación del Sistema Armonizado **1** (texto de la partida 21.06) y **6**.

Se adjunta al presente dictamen de clasificación arancelaria el informe técnico
DNR-DTA-JCC-FAFV-IF-2026-0376.

DISPOSICIONES FINALES:

Esta resolución se mantendrá vigente mientras permanezcan los hechos o las circunstancias que la motivaron, las normas jurídicas en que se fundamentó, y la nomenclatura bajo la cual se emitió.

Notifíquese por parte de la Dirección de Secretaría General del SENA E el contenido de la presente resolución conforme a los datos registrados por el usuario que constan en la petición adjunta en documentos asociados del presente Quipux.

La presente Resolución entrará en vigencia a partir de su notificación al solicitante, sin perjuicio de su publicación en el Registro Oficial.

Encárguese a la Dirección de Secretaria General del Servicio Nacional de Aduana del Ecuador formalizar las diligencias necesarias para publicar las resoluciones anticipadas en el Registro Oficial, la gaceta tributaria y en el portal web del Servicio Nacional de Aduana del Ecuador, **respetando las condiciones de confidencialidad a las que se refiere el artículo 5 de la Resolución N° SENA E-SENA E-2022-0011-RE.**

Documento firmado electrónicamente

Abg. David Andres Salazar Lopez
SUBDIRECTOR GENERAL DE NORMATIVA ADUANERA

Anexos:

- dnr-dta-jcc-fafv-if-2026-0376-signed-signed-signed-signed.pdf

Copia:

Señor Magíster
Luis Felipe Cedeño Puga
Director Nacional de Gestión de Riesgo y Técnica Aduanera

Señor Ingeniero
Luis Miguel Andino Montalvo
Director de Técnica Aduanera

Señorita
María Gabriela Hinojosa Muñiz
Directora Secretaría General

fafv/mvot/lmam/lfcv



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**DAVID ANDRES
SALAZAR LOPEZ**

**RESOLUCIÓN No. SEPS-IGT-IGS-IGJ-INSESF-INR-INGINT-INSEPS-2026-0157**

FREDDY ALFONSO MONGE MUÑOZ
INTENDENTE GENERAL TÉCNICO

CONSIDERANDO:

Que el artículo 283 de la Constitución de la República del Ecuador establece que: “... *El sistema económico es social y solidario; reconoce al ser humano como sujeto y fin; propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza; y tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir.*

El sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine. La economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios”.

Que el artículo 309 de la Constitución de la República señala: “*El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones”;*

Que el artículo 52 de la Constitución de la República del Ecuador señala que “*Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.*

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.”;

Que el artículo 213 de la Constitución de la República del Ecuador señala que “*Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general...”;*

- Que los numerales 1 y 7 del artículo 62, en concordancia con el inciso segundo del artículo 74 del Libro 1 del Código Orgánico Monetario y Financiero, determinan como funciones de la Superintendencia de Economía Popular y Solidaria ejercer la vigilancia, auditoría, control y supervisión de las disposiciones de dicho Código y de las regulaciones dictadas por la Junta de Política y Regulación Financiera y Monetaria, en lo que corresponde a las actividades financieras ejercidas por las entidades que conforman el sector financiero popular y solidario; así como velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y vigilar que cumplan las normas que rigen su funcionamiento, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, que permitan determinar su situación económica y financiera, evaluar la calidad y control de la gestión de riesgos y verificar la veracidad de la información que generan;
- Que el último inciso del artículo 62 del aludido Código determina que, para el cumplimiento de sus funciones, la Superintendencia podrá expedir las normas en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Financiera y Monetaria;
- Que los incisos segundo, tercero y quinto del artículo 74 del mencionado Código, establecen: “(...) *A la Superintendencia le compete el control de las entidades del sector financiero popular y solidario acorde a lo determinado en este Código. La Superintendencia de Economía Popular y Solidaria, en su organización, funcionamiento y funciones de control y supervisión del sector financiero popular y solidario, se regirá por las disposiciones de este Código y la Ley Orgánica de Economía Popular y Solidaria.*
- La Superintendencia de Economía Popular y Solidaria, además de las atribuciones que le otorga la Ley Orgánica de Economía Popular y Solidaria, tendrá las funciones determinadas en los artículos 71 y 62 excepto los numerales 19 y 28, y el numeral 10 se aplicará reconociendo que las entidades de la economía popular y solidaria tienen capital ilimitado. Los actos expedidos por la Superintendencia de Economía Popular y Solidaria gozarán de la presunción de legalidad y se sujetarán a lo preceptuado en la normativa legal vigente, respecto de su impugnación, reforma o extinción”;*
- Que el artículo 163 del referido Código determina que las cooperativas de ahorro y crédito, las cajas centrales, las asociaciones mutualistas de ahorro y crédito para la vivienda y las empresas de servicios auxiliares del sistema financiero calificadas por la Superintendencia de Economía Popular y Solidaria en el ámbito de su competencia, entre otras, forman parte del sector financiero popular y solidario;

- Que el artículo 444 del Código Orgánico Monetario y Financiero determina que las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Financiera y Monetaria y al control de la Superintendencia de Economía Popular y Solidaria, quienes en las políticas que emitan tendrán presente la naturaleza y características propias del sector financiero popular y solidario;
- Que la Ley Orgánica de Economía Popular y Solidaria, en el numeral 6 del artículo 132, establece que las organizaciones que conforman la Economía Popular y Solidaria podrán utilizar medios de pago complementarios, sea a través de medios físicos o electrónicos, para facilitar el intercambio y la prestación de bienes y servicios, dentro de las prescripciones establecidas en la Ley, su Reglamento y las regulaciones que para el efecto emita el órgano regulador competente;
- Que el artículo 146 de la Ley antes invocada establece: *"Superintendencia de Economía Popular y Solidaria.- El control de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario estará a cargo de la Superintendencia de Economía Popular y Solidaria, que se crea como organismo técnico, con jurisdicción nacional, personalidad jurídica de derecho público, patrimonio propio y autonomía administrativa y financiera y con jurisdicción coactiva.- La Superintendencia tendrá la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales"*;
- Que el literal b del artículo 147 de la Ley ibidem, determina: *"La Superintendencia, tendrá las siguientes atribuciones que las ejercerá de manera desconcentrada: Velar por la estabilidad, solidez y correcto funcionamiento de las instituciones sujetas a su control"*;
- Que los literales b) y g) del artículo 151 *ejusdem* establecen como atribuciones del Superintendente de Economía Popular y Solidaria dictar las normas de control; y, delegar algunas de sus facultades, siempre en forma concreta y precisa, a los funcionarios que juzgue del caso;
- Que la Ley Orgánica de Protección de Datos Personales establece el marco jurídico aplicable al tratamiento de datos personales, comprendiendo la observancia de principios, el respeto de los derechos de los titulares y la adopción de medidas de seguridad adecuadas, de conformidad con la normativa vigente;
- Que los numerales 1 y 8 del artículo 290 de la Sección XIV *"Norma de Servicios Financieros de las Entidades del Sector Financiero Popular y Solidario"*, del Capítulo XXXVI *"Sector Financiero Popular y Solidario"*, del Título II *"Sistema Financiero Nacional"*, del Libro I *"Sistema Monetario y Financiero"* de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, definen a los canales como los medios a través de los cuales las entidades atienden a sus socios, clientes o usuarios que solicitan un servicio financiero, o aquellos mecanismos mediante los cuales se hace efectiva la contraprestación de los

- servicios aceptados; y al servicio financiero como las actividades ejecutadas por las entidades para satisfacer las necesidades de sus socios, clientes o usuarios;
- Que el artículo 298 de la referida Sección establece que los servicios financieros con cargo diferenciado constarán en un catálogo administrado por la Superintendencia de Economía Popular y Solidaria y que las entidades podrán solicitar a este organismo de control la autorización para su prestación; mientras que aquellos servicios financieros con cargo diferenciado que no consten en dicho catálogo serán autorizados por la Junta de Política y Regulación Financiera y Monetaria, sobre la base de los informes remitidos por la Superintendencia;
- Que el artículo 9 de la *“Norma que regula los requisitos y el procedimiento para la autorización de servicios financieros a entidades del sector financiero popular y solidario bajo control de la Superintendencia de Economía Popular y Solidaria”* contenida en la Resolución No. SEPS-IGT-IGS-INSESF-INSEPS-INGINT-2021-0657, de 6 de octubre de 2021, emitida por este Organismo de Control, determina que las entidades podrán prestar servicios financieros mediante canales electrónicos, siempre que aseguren niveles adecuados de calidad y cumplan las medidas de seguridad aplicables; y dispone expresamente que la implementación de dichos canales no requiere autorización de la Superintendencia, sin perjuicio del cumplimiento de los requisitos técnicos, operativos y de control previstos en la normativa correspondiente;
- Que mediante Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 de 14 de abril de 2023, la Superintendencia de Economía Popular y Solidaria expidió la norma de control aplicable a las seguridades en el uso de transferencias electrónicas y canales electrónicos para las entidades financieras bajo su control;
- Que la evolución de los canales electrónicos y de las tecnologías utilizadas para la prestación de servicios financieros ha generado nuevos escenarios de riesgo relacionados con fraude electrónico, suplantación de identidad, accesos no autorizados, vulnerabilidades tecnológicas e incidentes de seguridad de la información, lo que hace necesario actualizar y fortalecer las medidas de autenticación, monitoreo, prevención, respuesta y protección de los usuarios, así como los mecanismos destinados a garantizar la seguridad y continuidad de los servicios financieros;
- Que en virtud de la Resolución No. CPCCS-PLE-SG-042-E-2024-0359-23-08-2024, emitida por el Pleno del Consejo de Participación Ciudadana y Control Social el 23 de agosto de 2024, el Pleno de la Asamblea Nacional posesionó como Superintendente de Economía Popular y Solidaria a la señorita magíster Christina Ivonne Murillo Navarrete, el 3 de septiembre de 2024;
- Que conforme consta en el literal j) del numeral 1.2.1.2 “Gestión General Técnica”, del artículo 9 de la Resolución No. SEPS-IGT-IGS-IGD-IGJ-001 de 31 de enero de 2022, que contiene el Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Economía Popular y Solidaria, es atribución

y responsabilidad del Intendente General Técnico, dictar las normas de control, en el ámbito de su competencia; y,

Que con acción de personal No. 200 de 10 de febrero de 2025, la Intendente General de Desarrollo Organizacional, delegada de la señorita Superintendente de Economía Popular y Solidaria, nombró Intendente General Técnico al economista Freddy Alfonso Monge Muñoz.

En ejercicio de sus atribuciones legales y estatutarias, resuelve expedir la siguiente:

NORMA DE CONTROL DE SEGURIDADES EN EL USO DE CANALES ELECTRÓNICOS PARA LAS ENTIDADES FINANCIERAS DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

SECCIÓN I ÁMBITO, OBJETO Y DEFINICIONES

Artículo 1. Objeto.- La presente resolución tiene por objeto establecer el marco normativo y las medidas mínimas de seguridad de la información, ciberseguridad y gestión de riesgos tecnológicos que deberán implementar las entidades, organizaciones y compañías de servicios auxiliares que operen u ofrezcan productos y servicios financieros mediante canales electrónicos, ya sea a través de infraestructura tecnológica propia o mediante la utilización de servicios provistos por terceros; en todos los entornos tecnológicos, plataformas, infraestructuras y mecanismos tecnológicos mediante los cuales se recopile, procese, transmita, almacene, intercambie o gestione información relacionada con productos, servicios, operaciones o transacciones financieras, así como a los mecanismos de autenticación, autorización, procesamiento y registro de dichas operaciones; incluyendo, entre otros: banca electrónica, banca móvil, aplicaciones transaccionales, canales digitales de autoservicio, interfaces de programación de aplicaciones (APIs) asociadas a servicios financieros, cajeros automáticos, tarjetas con chip de crédito y débito, tarjetas virtuales y/o tokenizadas, pagos inalámbricos seguros, dispositivos móviles, y cualquier otro canal tecnológico utilizado para la prestación de servicios financieros digitales.

Artículo 2. Ámbito.- La presente norma es aplicable a las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales, en adelante entidad o entidades, organizaciones y compañías de servicios auxiliares del sector financiero popular y solidario bajo control de la Superintendencia de Economía Popular y Solidaria que operen y ofrezcan servicios a través de canales electrónicos.

Artículo 3. Definiciones.- Los términos utilizados en la presente norma tendrán el siguiente significado:

1. **Activos de información críticos:** Son aquellos que presentan un riesgo ya que se encuentran directamente asociados a las actividades de las entidades o a la información personal sujeta a sigilo de los socios.
2. **Actualización forzosa o actualización obligatoria por seguridad:** Mecanismo técnico implementado por la entidad que impide el acceso a los servicios financieros desde una versión desactualizada de una aplicación o canal electrónico.
3. **Administrador del convenio de asociación:** Es la entidad que proporciona servicios a los intervinientes del convenio de asociación y que se encarga de la representación legal y correcta implementación del mismo.
4. **Alertas intradía:** Notificaciones automáticas generadas en tiempo real o en intervalos frecuentes durante la misma jornada operativa para reportar eventos financieros o de seguridad.
5. **Anonimización de datos:** Proceso mediante el cual se eliminan o modifican los identificadores directos e indirectos de una base de datos, de forma que se impida la identificación o reidentificación de una persona natural sin esfuerzos desproporcionados, garantizando que los datos no puedan ser asociados a un usuario específico.
6. **Autenticación de múltiples factores:** Es la combinación de al menos dos factores de distinta naturaleza: algo que el usuario conoce, algo que posee o algo que es, para verificar su identidad. Toda autenticación fuerte es, además, una autenticación multifactor, donde el usuario verifica su identidad tantas veces como factores se combinan.
7. **Autenticación fuerte:** Protocolo que exige al menos dos factores de verificación distintos (algo que sé, algo que tengo o algo que soy) para otorgar acceso.
8. **Autenticar:** Proceso, dispositivo o sistema utilizado para la comprobación de credenciales de acceso y la verificación de la identidad de un usuario.
9. **Autorización de accesos:** Acto por el cual se permite acceder a los usuarios a repositorios, almacenamientos digitales restringidos, a distintos equipos y/o servicios, después de haber superado el proceso de autenticación.
10. **Banca en línea:** Canal digital asociado a cuentas de depósito, líneas de crédito o cuentas de ahorro con requisitos simplificados, que utiliza un portal transaccional para tener acceso a servicios y transacciones financieras.
11. **Banca Móvil:** Canal digital que utiliza un aplicativo móvil para tener acceso a servicios y transacciones financieras.
12. **Banca Telefónica:** Canal digital para tener acceso a servicios y transacciones financieras a través de llamadas a los centros de atención telefónica.
13. **Billeteras digitales (Wallet):** Interfaz o software que permite a los usuarios realizar transferencias o transacciones en dinero, divisas valoradas y pagos de manera digital.
14. **Biometría:** Tecnología de autenticación basada en características físicas o conductuales únicas, como huella dactilar, reconocimiento facial o patrón de iris.
15. **Bloqueo preventivo:** Restricción temporal de una cuenta o canal electrónico activado automáticamente ante la detección de actividades inusuales o sospechosas.
16. **Botón de pánico:** Función de emergencia en una interfaz que permite al usuario reportar un fraude inmediato o bloquear sus servicios ante una amenaza detectada.

17. **Cajero automático o ATM (*Automated Teller Machine*):** Es una máquina expendedora y/o receptora de dinero que utiliza tarjetas con chip, claves u otros medios electrónicos sin que se requiera la presencia del personal de la entidad financiera, con las que también se puede realizar transferencias electrónicas, pagos y recargas de servicios tanto públicos como privados, entre otros.
18. **Canales electrónicos o digitales:** Se refieren a todas las vías o formas a través de las cuales los usuarios pueden efectuar transacciones con las entidades financieras, mediante el uso de elementos o dispositivos electrónicos o tecnológicos utilizando tarjetas, teléfonos móviles, programas de cómputo, aplicaciones en línea, entre otros.
19. **Centros de atención no presenciales:** Son plataformas centralizadas donde se gestiona la comunicación entre una entidad y sus socios, clientes o usuarios, sin requerir la presencia física de ninguna de las partes. Operan a través de canales remotos como telefonía, internet, correo electrónico, mensajería, redes sociales o cualquier medio telemático.
20. **Certificado digital:** Documento electrónico firmado por una autoridad de certificación que vincula una clave pública con una identidad, garantizando integridad y no repudio.
21. **Cifrado:** Proceso mediante el cual la información o archivos son codificados en forma lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarla, verla o copiarla.
22. **Componentes de terceros o bibliotecas de terceros:** Fragmentos de software, librerías, *frameworks*, SDKs, módulos o cualquier otro bloque de código desarrollado por un proveedor externo a la entidad, que es incorporado en las aplicaciones o sistemas de canales electrónicos para proveer funcionalidades específicas, sin que la entidad tenga control directo sobre su desarrollo original.
23. **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
24. **Convenio de asociación:** Es un acto jurídico que tiene fines comunes para las partes, es decir, beneficios recíprocos en cuanto a la prestación de servicios financieros o complementarios y que se formalizan en los acuerdos firmados entre dos o más entidades o compañías de servicios auxiliares que se encuentran en funcionamiento, para la ampliación o prestación de uno o varios servicios específicos.
25. **Datos sintéticos:** Conjuntos de datos generados artificialmente que imitan la estructura y propiedades estadísticas de los datos reales, pero que no contienen información de personas, cuentas o transacciones verdaderas, siendo utilizados exclusivamente en entornos de pruebas, desarrollo o capacitación.
26. **Debida diligencia en seguridad (de terceros):** Proceso sistemático de evaluación y verificación previa a la contratación de un proveedor de servicios tecnológicos, que incluye el análisis de sus prácticas de seguridad de la información, certificaciones, historial de incidentes, controles de acceso, ubicación de datos, planes de continuidad, y su capacidad para cumplir con la presente norma y la normativa aplicable.
27. **Desensibilización de datos (*Data masking*):** Técnica de protección de datos que reemplaza información sensible original por caracteres genéricos o ficticios,

- preservando el formato y ciertas propiedades funcionales para permitir pruebas o análisis, pero impidiendo la lectura directa de los datos reales.
28. **Disponibilidad:** Acceso a la información en el tiempo y forma en que ésta sea requerida.
 29. **Entorno de ejecución comprometido (*root o jailbreak*):** Estado de un dispositivo móvil en el que se han removido las restricciones impuestas por el fabricante o sistema operativo, permitiendo al usuario obtener privilegios de administrador (*root* en Android, *jailbreak* en iOS), lo que incrementa significativamente el riesgo de ejecución de software malicioso, modificación de la aplicación y bypass de controles de seguridad.
 30. **Exfiltración:** Cuando se incurre en la copia, transferencia o recuperación no autorizadas de datos de un servidor o del ordenador de un individuo.
 31. **Firma criptográfica del dispositivo (Indicador criptográfico del dispositivo):** Es un sello criptográfico generado por el hardware (usualmente mediante un chip de seguridad o TPM) para autenticar su identidad y garantizar que los datos enviados no han sido alterados.
 32. **Fuerza mayor o caso fortuito:** Se refieren al imprevisto que no es posible controlar, tales como: huelgas, paros, guerras, actos de vandalismo, terrorismo, manifestaciones, conmoción civil, terremotos, incendios, inundaciones actos de autoridad ejercidos por funcionario público, u otros similares. conforme a lo dispuesto en el artículo 30 del Código Civil.
 33. **Hardening:** Proceso de asegurar un sistema mediante la reducción de su superficie de ataque, eliminando funciones, puertos y servicios innecesarios.
 34. **Incidente de seguridad:** Evento adverso confirmado que compromete la confidencialidad, integridad o disponibilidad de la información o los servicios digitales.
 35. **Información:** Es cualquier forma de registro físico, electrónico, óptico, magnético o de otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.
 36. **Ingeniería inversa de software:** Proceso de análisis de una aplicación o sistema para descubrir su código fuente, estructura, algoritmos, componentes o lógica interna, con el fin de comprender su funcionamiento, extraer información protegida, modificar su comportamiento o identificar vulnerabilidades, sin contar con la autorización del titular de los derechos.
 37. **Integridad:** Es la garantía de mantener la calidad y exactitud de la información.
 38. **Medios de pagos digitales:** Son los mecanismos electrónicos o digitales, definidos por el organismo regulador, utilizados para la transferencia de recursos y/o pagos.
 39. **No repudio:** Propiedad de las comunicaciones que garantiza la participación de las partes en una transacción.
 40. **Notificación Push:** Mensaje enviado desde un servidor a una aplicación móvil que aparece automáticamente en el dispositivo para informar o validar operaciones.
 41. **Ofuscación de código:** Técnica de transformación del código fuente o ejecutable de una aplicación que lo hace difícil de entender, analizar o modificar por humanos o herramientas automatizadas, sin alterar su funcionalidad, con el

- propósito de dificultar la ingeniería inversa, el robo de propiedad intelectual o la identificación de vulnerabilidades.
42. **OTP (*One-time password*)**: Contraseña de un solo uso con una temporalidad asociada para su vigencia.
 43. **Perfil de riesgo**: Evaluación basada en el comportamiento, ubicación y hábitos del usuario para determinar la probabilidad de fraude en una sesión o transacción.
 44. **Pruebas de penetración**: Ciberataques simulados y controlados contra un sistema para identificar vulnerabilidades explotables antes de que lo haga un atacante real.
 45. **Quiosco**: Son dispositivos de autoservicio que brindan a los usuarios acceso a información.
 46. **SDK (*Software Development Kit*)**: Conjunto de herramientas, bibliotecas, documentación y ejemplos de código proporcionado por un tercero para facilitar el desarrollo de aplicaciones que integran servicios específicos (como pasarelas de pago, autenticación, analítica, notificaciones), el cual debe ser evaluado en cuanto a su seguridad antes de su inclusión en los canales electrónicos.
 47. **Seguridad de la información**: Son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados.
 48. **Servicios críticos de terceros**: Aquellos servicios tecnológicos externalizados cuya interrupción, fallo o vulneración afectaría de manera significativa la disponibilidad, integridad o confidencialidad de los servicios financieros ofrecidos a través de canales electrónicos, o pondría en riesgo los datos de los usuarios.
 49. **Servicios financieros electrónicos**: Son servicios financieros prestados por medios digitales, que se pueden brindar por canales presenciales o no presenciales.
 50. **Sistemas de audio respuesta o IVR (*Interactive voice response*)**: Sistema automatizado de respuesta interactiva, orientado a entregar o capturar información a través del teléfono, permitiendo el acceso a servicios de información.
 51. **Terminales de punto de venta (POS)**: Dispositivos electrónicos que posibilitan transmitir las instrucciones de pagos, realizadas a través de tarjetas y otros dispositivos electrónicos.
 52. **Terminales electrónicos**: Dispositivos conectados en línea a una plataforma tecnológica de servicios financieros, mismos que pueden ser fijos o móviles, tales como ATM, POS, PIN Pad (teclado para el ingreso del número de identificación personal), App (aplicación), entre otros.
 53. **Tiempo real**: Se refiere a las transacciones que se ejecutan de manera inmediata y que sus resultados de ejecución son visualizados en el instante que se realizan.
 54. **Token**: Dispositivo físico o software que genera claves dinámicas temporales (OTP) para validar la identidad del usuario en una transacción.
 55. **Transacción electrónica**: Es cualquier actividad que involucra la transferencia de información digital para propósitos específicos.
 56. **Transferencia electrónica**: Transacciones de fondos, realizadas por cualquier usuario habilitado para este fin, haciendo uso de los diferentes terminales electrónicos; las transacciones pueden referirse a: órdenes de cobro, órdenes de pago, abonos a cuentas, débitos en puntos de venta, retiros de dinero, entre otros.

57. **Usuarios:** Son los socios, clientes o terceros que utilizan cualquier servicio financiero prestado por las entidades.
58. **Verificación de integridad de la aplicación:** Mecanismo de seguridad que permite comprobar periódicamente que el código y los recursos de una aplicación no han sido modificados, alterados o reemplazados desde su última versión oficial aprobada, detectando manipulaciones no autorizadas (por ejemplo, mediante la adición de código malicioso) y pudiendo tomar acciones como la denegación de servicio o la notificación al usuario.
59. **Vinculación de dispositivo (*Device Binding*):** Es un control de seguridad que enlaza la identidad digital de un usuario con un hardware específico mediante un identificador único criptográfico.

SECCIÓN II

MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN EN LOS CANALES ELECTRÓNICOS

Artículo 4. Medidas de seguridad de la información.- Las entidades deberán contar con las medidas de seguridad de la información en los canales electrónicos, para poder brindar servicios financieros, con la implementación de al menos las siguientes medidas:

1. Precautelar la integridad, disponibilidad y confidencialidad de los registros e información de los usuarios;
2. Establecer medidas de control y de alerta temprana con el fin de prevenir la materialización de posibles riesgos;
3. Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los terminales y sistemas usados para transacciones electrónicas;
4. Contar con privilegios de autorización, medidas de autenticación y controles de acceso lógico que contemplen por lo menos dos de los tres factores: “algo que se sabe, algo que se tiene, o algo que es”. Las entidades podrán implementar otros mecanismos adicionales de seguridad con el fin de precautelar la transacción;
5. Implementar múltiples factores de autenticación, que combinen al menos dos factores de distinta naturaleza en cada plataforma en línea a la que accede el usuario, en todas sus cuentas;
6. Requerir mecanismos de autenticación de múltiples factores para el registro y modificación de la información de contacto, como número de celular o correo electrónico, cuando los usuarios lo realicen por cualquier canal presencial o no presencial;
7. Para el uso de los factores de autenticación, las entidades deberán cumplir, al menos, con lo siguiente:
 - a. Mantener procedimientos que avalen la seguridad de la información de sus usuarios durante la generación, custodia, distribución, asignación y reposición o sustitución de dichos factores;
 - b. No divulgar o acceder a la información protegida en relación con los factores de autenticación;

- c. Informar a sus usuarios que la entidad no requerirá bajo ningún medio y bajo ninguna condición la información sobre sus factores de autenticación; y,
 - d. Las entidades no podrán solicitar información parcial o completa de las contraseñas del usuario.
8. Capacitar e informar a los usuarios sobre los riesgos derivados del uso de canales electrónicos; y sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de estos.

Artículo 5. Claves digitales y validación en la aplicación móvil.- Se establece la obligatoriedad de que las entidades pongan a disposición de los usuarios cualquiera de los siguientes mecanismos de seguridad para el uso de canales digitales de acuerdo con el nivel de criticidad que cada entidad determine:

1. Token Digital Incorporado: La aplicación móvil oficial deberá contar con un generador de claves dinámicas (OTP) y/o un sistema de validación criptográfica, independiente de la red SMS.
2. Notificaciones Push de Confirmación: Para toda transacción que implique un movimiento de fondos o el registro de un nuevo beneficiario, la entidad deberá enviar una notificación "*push*" a la aplicación móvil del usuario registrado, solicitando su confirmación o rechazo expreso.
3. Biometría: Se deberá habilitar la autenticación biométrica (huella dactilar o reconocimiento facial) como segundo factor de validación para el acceso a la aplicación y la autorización de transacciones significativas (garantizando que la información biométrica no sea almacenada ni quede a cargo de la entidad responsable del servicio, de conformidad con la normativa de protección de datos personales).

Artículo 6. Vinculación de dispositivos y alertas intradía.- Las entidades deberán implementar sistemas de registro y firma digital que permitan identificar los equipos desde los cuales opera el usuario y analizar sus horarios habituales de conexión y saldos promedio. Cualquier intento de acceso o transacción desde un dispositivo no registrado deberá:

1. Ser registrado mediante un proceso adecuado que permita verificar la identidad del titular de la cuenta; o ser bloqueado, en caso de que dicha comprobación no sea exitosa, requiriendo pasos adicionales de verificación.
2. Generar una alerta inmediata y simultánea al usuario a través de la aplicación móvil, correo electrónico y SMS, informando del intento y las instrucciones a seguir en caso de no haber sido el iniciador; y,
3. Vinculación segura del usuario al dispositivo y criptográfica a la aplicación móvil transaccional que contemple al menos:
 - a. Uso de claves digitales almacenadas de forma segura en el dispositivo;
 - b. Validación del estado de seguridad del dispositivo; e
 - c. Invalidación automática de la vinculación ante:
 - i. Cambio de tarjeta SIM;
 - ii. Reinstalación de la aplicación móvil; y
 - iii. Detección de alteraciones en la seguridad del dispositivo;

Artículo 7. Medidas de Seguridad Tecnológicas.- Las entidades deberán contar con las medidas de seguridad tecnológicas en los canales electrónicos, al momento de brindar servicios financieros, con al menos las siguientes medidas:

1. Contar como parte de su infraestructura tecnológica, con protocolos de seguridad que realicen las funciones de autenticación y validación de los usuarios; autorización y uso de los recursos o servicios, así como el registro de la actividad de los usuarios y su perfilamiento para el respectivo seguimiento;
2. Cifrar la información crítica en reposo o en tránsito, incluso en dispositivos electrónicos y de almacenamiento, extraíbles o móviles; debiendo asegurarse de que los protocolos utilizados sean seguros y se guíen por estándares y buenas prácticas internacionales;
3. Contar con desarrollos de software seguros y adecuados, conforme lo dispuesto en la Norma de Control de Seguridad de la Información emitida por esta Superintendencia;
4. El software que se utilice para las transacciones deberá registrar al menos: accesos, nivel de transaccionalidad, límites individuales de transaccionalidad, perfiles de usuarios financieros, entre otra información disponible para valoración. Deberán generar reportes sobre dicha información;
5. Establecer perfiles de comportamiento del uso de los canales por parte de los socios a través del establecimiento de patrones de uso para la emisión de alertas y acciones oportunas ante indicadores sospechosos;
6. Registrar las direcciones IP y/o números de telefonía móvil desde las que se realizan las transacciones en los canales electrónicos, las cuales serán utilizadas para establecer el origen de la transacción y verificar la existencia de las autorizaciones pertinentes para la misma;
7. Mantener sincronizados todos los relojes de sus sistemas informáticos, contables, de información y los dispositivos que integran la plataforma de canales electrónicos;
8. Disponer de canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares internacionales vigentes sobre la materia;
9. Utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos; y garantizar que dicha información permanezca cifrada en todo momento;
10. Incorporar procesos periódicos de renovación de clave, con una frecuencia de al menos una vez al año, para el acceso a los sistemas de canales electrónicos por parte de los usuarios;
11. Implementar o actualizar las herramientas y mecanismos para monitorear redes y demás infraestructura tecnológica que permitan detectar oportunamente eventos que atenten contra la seguridad de la información, actividad o comportamientos inusuales;
12. Contar con procesos ágiles para adquirir, probar e instalar parches para los componentes de la infraestructura tecnológica, de tal forma que los parches se mantengan actualizados; y evitar el uso de aplicaciones, sistemas operativos y manejadores de bases de datos sin el respaldo del fabricante o proveedor de actualizaciones de seguridad;

13. Contar con programas o software actualizados para detectar, proteger y eliminar software malicioso, así como revisar los ajustes de configuración y la vigencia de las licencias para garantizar el nivel de protección esperado;
14. Contar con herramientas para prevenir la suplantación de identidad ante amenazas basadas en phishing, spam, spear-phishing, entre otros; y considerar la idoneidad de estas herramientas, de tal manera que sean consistentes con el tamaño de la entidad. Las entidades deberán contar con programas de capacitación constante para sus empleados sobre este tipo de amenazas. Las entidades deberán contar con herramientas de prevención de pérdida de datos para tener una visibilidad de los efectos ante dicho evento, de tal forma que se fortalezca la detección y prevención de la fuga de datos;
15. Adecuar los sistemas y demás componentes de la infraestructura tecnológica, para generar la capacidad de contar con un registro de información que permita detectar de forma activa e investigar incidencias, asegurándose de que los registros de actividades estén disponibles para su análisis cuando sea necesario;
16. Mantener un proceso continuo de aplicación de técnicas que se enfoquen en la configuración segura de hardware y software (*hardening*), para la matriculación o enrolamiento de los dispositivos electrónicos de los usuarios que se utilicen en la prestación de servicios financieros a través de canales electrónicos;
17. Establecer procedimientos para monitorear, controlar y emitir alertas en línea, que informen oportunamente sobre el estado de los canales electrónicos;
18. Establecer procedimientos que incluyan al menos:
 - a. Notificar inmediatamente vía aplicación móvil (app) y correo electrónico cada inicio de sesión y movimiento, sin excepción.
 - b. Bloquear preventivamente el acceso cuando se presenten transacciones desde una IP inusual o un dispositivo nuevo no enrolado previamente, sin que se hubiera podido identificar adecuadamente la identidad del socio.
 - c. Permitir la opción de restringir transferencias de alto valor por las primeras 12 a 24 horas, en caso de identificarse cambios de clave, ajustes de límites de transferencias o ajustes en beneficiarios; y,
19. Mantener un inventario actualizado de todas las bibliotecas, frameworks, SDKs y componentes de terceros incorporados en las aplicaciones y canales electrónicos, incluyendo su versión y origen. Las entidades deberán:
 - a. Realizar análisis de vulnerabilidades conocidas sobre dichos componentes al menos trimestralmente, y antes de cada publicación o actualización significativa;
 - b. Sustituir o parchear aquellos componentes que presenten vulnerabilidades de severidad alta o crítica;
 - c. Eliminar componentes no utilizados o en desuso (*dead code*) de las aplicaciones en producción.

Artículo 8. Transacciones en canales electrónicos.- Las entidades que ofrezcan sus servicios en canales electrónicos deberán aplicar buenas prácticas para la administración del riesgo operacional y estándares internacionales, poniendo énfasis en:

1. Reconocer la validez de las operaciones y transacciones realizadas;

2. Establecer límites, los cuales pueden ser personalizados por el usuario para cada operación y transacción autorizada;
3. Imposibilitar que el valor de la transferencia supere el saldo disponible o el límite establecido, ya sea por la entidad o el usuario;
4. Permitir que el saldo de la cuenta del usuario se consulte, verifique, acredite o debite en tiempo real;
5. Permitir al usuario realizar consultas de los movimientos realizados a través de cualquier dispositivo electrónico, informando la temporalidad máxima a la que puede acceder la consulta;
6. Ofrecer a los usuarios los mecanismos necesarios para que, a través de métodos de autenticación fuerte, personalicen las condiciones bajo las cuales desean realizar sus transacciones monetarias mediante los diferentes canales electrónicos;
7. Establecer procedimientos de control y mecanismos que permitan determinar el perfil de riesgo de las transacciones realizadas por los usuarios, que impliquen movimiento de dinero en el uso de canales electrónicos; lo que deberá ser notificado inmediatamente al usuario mediante mensajería móvil, correo electrónico, u otro mecanismo;
8. Incorporar procedimientos de bloqueo de los canales electrónicos cuando se presenten eventos inusuales que adviertan situaciones fraudulentas, o después de un número máximo de tres intentos de acceso fallido; lo cual se debe notificar inmediatamente al usuario a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura;
9. Establecer procesos y mecanismos automáticos para bloquear preventivamente el acceso a cualquiera de los canales electrónicos, en los siguientes casos:
 - a. Cuando los sistemas de monitoreo detecten comportamiento transaccional inusual o irregular de acuerdo con el perfil del usuario;
 - b. Cuando los sistemas de seguridad detecten un ataque informático que comprometa los datos o información de los usuarios; y,
 - c. Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del usuario.
10. Poner a disposición de los usuarios una línea telefónica para emergencias con atención las veinticuatro (24) horas, siete (7) días a la semana; adicionalmente podrán contar con accesos directos de atención al usuario de otra naturaleza que permitan mantener un registro del día y la hora en las cuales se dio el inicio de contacto del usuario;
11. Los centros de atención no presenciales al usuario, para validar la identidad de la persona que está siendo atendida, deberán implementar mecanismos que verifiquen que el usuario es quien dice ser;
12. Conservar para disponibilidad del usuario el registro de las transacciones electrónicas como mínimo durante doce (12) meses; mismo que deberá contener al menos lo siguiente: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), identificación del usuario, RUC de la entidad de origen y de destino, número de transacción, código del terminal electrónico y el canal utilizado. Para transacciones por internet la dirección IP, ubicación geográfica aproximada y el proveedor de internet; para transacciones a través de sistemas de audio respuesta y para transacciones del servicio financiero móvil, el número de teléfono con el que se hizo la conexión; y,

13. Determinar la disponibilidad histórica de los registros de las transacciones electrónicas que superen los doce (12) meses del registro.

Artículo 9. Continuidad de operaciones.- El proceso de continuidad de operaciones de los sistemas utilizados por las entidades para las transferencias electrónicas, debe cubrir eventos fortuitos o de fuerza mayor; considerando el uso de equipos, sistemas y plataformas de respaldo a través de procedimientos de contingencia establecidos por las áreas del negocio.

Artículo 10. Planes de mitigación.- Las entidades deberán contar con planes de respuesta para mitigar el impacto ante un incidente de seguridad de la información. Estos planes deben ser probados para verificar la capacidad de respuesta e identificar brechas y oportunidades de forma continua.

Artículo 11. Notificación de incidentes de seguridad.- Las entidades deberán reportar a la Superintendencia de Economía Popular y Solidaria cualquier incidente de seguridad de la información que afecte o pueda afectar significativamente la confidencialidad, integridad o disponibilidad de los servicios financieros prestados a través de canales electrónicos, o que comprometa datos personales de los usuarios. El reporte inicial deberá efectuarse dentro de las veinticuatro (24) horas contadas desde que la entidad tenga conocimiento del incidente, siempre que se verifiquen criterios de materialidad relacionados con afectación a usuarios, interrupción relevante del servicio, compromiso de datos personales, pérdida económica, indisponibilidad del canal o impacto reputacional significativo.

El reporte deberá contener, al menos: descripción del incidente, fecha y hora de inicio, sistemas afectados, acciones de contención implementadas, número estimado de usuarios afectados, y medidas provisionales adoptadas. La entidad deberá presentar un informe detallado de causa raíz y plan de remediación dentro de los cinco (5) días hábiles posteriores al incidente.

SECCIÓN III

MEDIDAS DE SEGURIDAD ESPECÍFICAS POR CADA SERVICIO

Artículo 12. Cajeros automáticos, dispositivos móviles, quioscos y similares.- Las entidades que ofrezcan servicios a través de cajeros automáticos, dispositivos móviles, quioscos y similares por cuenta propia o a través de terceros deberán:

1. Verificar que la información de las claves no se almacene en ningún momento;
2. Verificar que los dispositivos utilizados para la autenticación del usuario cifren la información ingresada a través de ellos;
3. Implementar mecanismos internos de autenticación que permitan asegurar que el dispositivo se encuentre autorizado por la entidad y vinculado de manera única;
4. Verificar el cumplimiento de la normativa vigente relacionada con las seguridades físicas y electrónicas.

Artículo 13. Terminales de puntos de venta.- Las entidades que ofrezcan servicios a través de los terminales de puntos de venta por cuenta propia o a través de terceros, deben:

1. Exigir que los establecimientos procesen en presencia del usuario el pago de las transacciones efectuadas;
2. Asegurarse de que también procesen la información de otros medios de pago digitales y enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando las transacciones realizadas y sus modificaciones; y,
3. Establecer los mecanismos para confirmar que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta en los establecimientos comerciales, pertenezcan a la entidad o a terceros contratados por esta.

Artículo 14. Banca electrónica o banca móvil.- Las entidades que ofrezcan servicios de banca electrónica o banca móvil por cuenta propia o a través de terceros, deben:

1. Implementar mecanismos que permitan detectar la copia de los diferentes componentes de su sitio web;
2. Verificar constantemente que no sean modificados sus enlaces, suplantados sus certificados digitales, ni modificada indebidamente la resolución del sistema de nombres de dominio;
3. Implementar mecanismos de autenticación para el acceso a dicho servicio por parte de los usuarios, en donde el nombre de usuario y clave de acceso cumplan con las mejores prácticas de seguridad;
4. Validar o verificar la autenticidad del usuario a través de un canal distinto al de internet, o por medios biométricos, para establecer las condiciones personales bajo las cuales realizará y recibirá sus servicios y transacciones por internet, o modificará sus datos de contacto;
5. En los casos de inicio de sesión mediante banca móvil, la entidad deberá remitir un mensaje al usuario, a través de al menos dos medios electrónicos de los que disponga, tales como correo electrónico y/o mensajes de texto;
6. Enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando las transacciones realizadas;
7. Implementar mecanismos de protección del código fuente de la aplicación móvil, incluyendo al menos: ofuscación de código, detección de entornos de ejecución comprometidos (*root/jailbreak*), verificación de integridad de la aplicación en tiempo de ejecución, y resistencia a la ingeniería inversa y a la reingeniería. Las entidades deberán actualizar dichos mecanismos periódicamente conforme a la evolución de las amenazas; y,
8. Establecer un mecanismo que permita a la entidad exigir al usuario la actualización obligatoria de la aplicación móvil cuando se identifiquen vulnerabilidades críticas en versiones anteriores, o cuando la versión en uso haya quedado fuera de soporte. Dicho mecanismo deberá impedir el acceso a los servicios financieros desde versiones no actualizadas, previa notificación al usuario con una antelación razonable.

Artículo 15. Banca telefónica a través de IVR.- Además de lo especificado en las medidas de seguridad operativa, para el uso del servicio de banca telefónica los usuarios deberán autenticar su identidad a través del IVR con un factor de autenticación adicional como una contraseña que solo el usuario conozca.

SECCIÓN IV DE LOS SERVICIOS OFRECIDOS A LOS USUARIOS

Artículo 16. Medidas de seguridad en la afiliación de los usuarios a los productos o servicios financieros.- Para la afiliación de los usuarios a los productos o servicios financieros por medio de canales electrónicos, las entidades deberán al menos:

1. Implementar la aceptación de contratos por medios digitales, utilizando múltiples factores de autenticación y del contenido aceptado, de conformidad con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
2. Implementar algoritmos y protocolos seguros, así como certificados digitales, los cuales deberán incluir el uso de técnicas de cifrado para las transacciones realizadas;
3. Implementar mecanismos de control y monitoreo que reduzcan la posibilidad de que los usuarios accedan a páginas web falsas y/o fraudulentas. En caso de materialización de eventos adversos, se deberán implementar mecanismos de mitigación;
4. Enviar a sus usuarios notificaciones, por al menos dos vías, tales como: mensajería de texto, correo electrónico u otros mecanismos reconocidos por el usuario; notificando al menos el acceso a la banca en línea, banca móvil, transacciones realizadas, productos financieros adquiridos y sus modificaciones;
5. Informar al usuario al inicio de cada sesión la fecha, hora, dirección IP y dispositivo del último ingreso al canal de banca electrónica; y,
6. Implementar mecanismos de autenticación al inicio de sesión de los usuarios, en donde el nombre de usuario debe ser distinto al número de cédula, número de pasaporte, u otro documento de identidad.

Artículo 17. Información al usuario.- Las entidades deberán informar a sus usuarios de forma escrita o a través de cualquier otro medio de comunicación previamente registrado y aceptado, al momento de activar por primera vez el uso de los canales electrónicos al menos lo siguiente:

1. Servicios ofrecidos y las responsabilidades de su uso;
2. Procedimientos para la afiliación, cancelación, suspensión y reactivación del servicio;
3. Límites de montos y transacciones a realizar;
4. Comisiones y tarifas por el uso del servicio, con su respectiva descripción;
5. Riesgos inherentes a su utilización;
6. Procedimiento para informar cualquier irregularidad o actividad potencialmente no reconocida o no autorizada y que haya sido detectada, ya sea por el usuario o por la entidad;

7. Procedimiento para la atención de consultas y reclamos de los usuarios;
8. Aceptación de responsabilidades por parte del usuario y la entidad;
9. Consejos para el adecuado uso de canales electrónicos por parte del usuario; y,
10. Información clara, transparente, comprensible y accesible sobre el tratamiento de los datos personales del usuario asociado a la activación y utilización de los canales electrónicos, que deberá incluir, al menos:

- a. Las finalidades específicas del tratamiento;
- b. La base legitimadora aplicable a cada finalidad;
- c. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible determinarlo, los criterios utilizados para establecer dicho plazo;
- d. Los derechos que corresponden al titular de los datos personales, incluidos los derechos de acceso, rectificación y actualización, eliminación y oposición, así como los demás reconocidos en la normativa vigente; y,
- e. Los canales y el procedimiento habilitados por la entidad para el ejercicio de los derechos del titular y, cuando corresponda, para la revocatoria del consentimiento.

La información prevista en este numeral deberá proporcionarse sin perjuicio de los demás contenidos exigidos por la normativa vigente en materia de protección de datos personales; y,

11. En todos los canales electrónicos, cuando corresponda, las entidades deberán proveer información al usuario, de acuerdo con lo siguiente:
 - a. Elementos que identifiquen que se encuentran utilizando plataformas tecnológicas y/o dispositivos electrónicos que pertenezcan a la entidad antes de ingresar los elementos de autenticación; y,
 - b. Una vez que el usuario verifique que se trata de una plataforma tecnológica, dispositivo electrónico, o canal digital oficial de la entidad e inicie una sesión segura, se deberán proporcionar de forma notoria y visible notificaciones al usuario, y proceder a la generación de registros internos de al menos la siguiente información:
 - i. Fecha, hora, dirección IP y dispositivo de su último inicio de sesión; y,
 - ii. Nombre, apellido u otro identificador único del usuario.

Artículo 18. Identificación del usuario al inicio de sesión.- Para permitir el inicio de sesión a los usuarios a través de los canales electrónicos, las entidades deberán solicitar y validar al menos lo siguiente:

1. Un identificador de usuario único y su contraseña o clave de acceso de acuerdo con las mejores prácticas internacionales; y,
2. El uso de un factor de autenticación adicional de distinta naturaleza al anterior.

Artículo 19. Verificación de la identidad de los usuarios.- Las entidades deberán implementar mecanismos de autenticación fuerte para verificar la identidad de los usuarios que accedan o realicen transacciones a través de canales electrónicos o digitales.

Dichos mecanismos deberán basarse en el uso de múltiples factores de autenticación que combinen, al menos, dos de los siguientes elementos: algo que el usuario conoce, algo que el usuario posee y algo que el usuario es.

Cuando los mecanismos de verificación de identidad, autenticación o seguridad incluyan procesos de perfilamiento de los usuarios, estos se realizarán exclusivamente con fines de prevención del fraude y protección de la seguridad de las operaciones y servicios financieros, de conformidad con la Ley Orgánica de Protección de Datos Personales y demás normativa aplicable. Las entidades deberán observar los principios de finalidad, pertinencia, minimización, proporcionalidad, transparencia y seguridad, y no podrán utilizar la información obtenida mediante el perfilamiento para fines distintos o incompatibles con aquellos que justificaron su tratamiento.

Para efectos de la presente norma, podrán utilizarse, entre otros, los siguientes mecanismos: contraseñas o claves secretas que solo el usuario conoce, preguntas de desafío, claves dinámicas de un solo uso —OTP—, dispositivos de autenticación, validaciones biométricas u otros mecanismos equivalentes que permitan verificar de manera segura la identidad del usuario.

Las entidades deberán considerar, al menos, los siguientes controles:

1. **Vinculación segura del dispositivo —Device Binding—:** Implementar mecanismos que permitan asociar el dispositivo utilizado por el usuario con su identidad digital, de forma que las credenciales o llaves digitales utilizadas para la autenticación se encuentren vinculadas al hardware del dispositivo mediante entornos seguros de ejecución, tales como módulos de seguridad del dispositivo o tecnologías equivalentes, evitando su clonación o reutilización en dispositivos no autorizados.
2. **Mecanismos seguros de aprobación de transacciones:** Implementar notificaciones seguras dentro de la aplicación o mecanismos equivalentes de aprobación de transacciones que permitan al usuario validar las operaciones desde la aplicación oficial de la entidad. Estos mecanismos deberán mostrar de forma clara los detalles relevantes de la transacción, tales como el monto, la cuenta de destino u otros datos pertinentes, con la finalidad de reducir el riesgo de fraude por ingeniería social o suplantación.
3. **Uso de mecanismos avanzados de autenticación:** Promover la implementación de estándares y tecnologías avanzadas de autenticación, tales como autenticación biométrica o mecanismos basados en estándares abiertos de autenticación segura, que reduzcan la dependencia de contraseñas compartidas y fortalezcan la protección contra fraudes y accesos no autorizados.
4. **Monitoreo basado en riesgos:** Implementar mecanismos de monitoreo transaccional y de autenticación adaptativa basados en riesgos, que permitan identificar comportamientos atípicos, cambios de dispositivo, variaciones en la ubicación geográfica u otras variables que puedan indicar posibles intentos de fraude. Estos mecanismos deberán revisarse y actualizarse, al menos, una vez al año.

Artículo 20. Métodos adicionales de autenticación.- Las entidades podrán establecer métodos adicionales de autenticación con el fin de reforzar las transacciones realizadas en canales electrónicos.

Las entidades podrán poner a disposición del usuario al menos un mecanismo que permita lo siguiente:

1. Obtener el historial de transacciones realizadas en los últimos 90 días, que como mínimo incluirá el número de referencia, monto, fecha, hora, tipo de transacción, tipo de producto y canal;
2. Un procedimiento para el desbloqueo de usuario y contraseña; y,
3. Un procedimiento para definir una nueva clave o contraseña.

Artículo 21. Uso de factores de autenticación.- Los sistemas de canales electrónicos de las entidades deberán requerir al menos dos factores de autenticación de distinta naturaleza para el inicio de sesión, de conformidad con los artículos 18 y 19. Estos mecanismos deberán aplicarse también para el acceso a los siguientes servicios:

1. Afiliación, desafiliación y registro de productos, servicios y transacciones programadas;
2. Utilización de productos y servicios;
3. Pagos de servicios, canje de beneficios, retiros o adelantos de efectivo, desactivación de productos, generación y cambios de contraseñas, transferencias electrónicas a terceros;
4. Actualización de datos de la ficha del usuario y límites para las transacciones a efectuar;
5. Consultas; y,
6. Transacciones ofrecidas a través de dispositivos de autoservicio.

Artículo 22. Inhabilitación del acceso.- Las entidades deberán inhabilitar inmediatamente el acceso a los servicios ofrecidos por canales electrónicos cuando el usuario o la propia entidad presuman que se puede ver afectada, o se ha visto afectada, la seguridad de los servicios financieros ofertados, debiendo las entidades contar con diferentes medios, tanto presenciales como digitales para tal efecto.

Artículo 23. Confirmación de transacción.- Las entidades deberán generar una confirmación inmediata al usuario, contando con mecanismos de no repudio, sobre las transacciones que se realicen por medio de canales electrónicos, mediante mensajes de texto a su dispositivo móvil u otro medio de comunicación registrado, que le servirá para determinar que la transacción se ha completado. Las confirmaciones relativas a movimientos de fondos, registro o modificación de beneficiarios, cambios de claves, variación de límites transaccionales, modificación de datos de contacto y demás operaciones críticas serán obligatorias e irrenunciables. Para operaciones no críticas, la entidad podrá permitir que el usuario configure sus preferencias de notificación, siempre que mantenga al menos un canal mínimo de alerta y que dicha configuración se encuentre debidamente documentada.

Asimismo, las entidades enviarán vía electrónica la notificación del estado de la transacción que hubiere sido ejecutada, la cual deberá incluir, como mínimo, el texto: “transacción exitosa”, detallando fecha, hora, tipo de producto, tipo de transacción, número de referencia y monto de la operación, entre otra información pertinente. En caso de que la transacción no sea exitosa, enviarán un mensaje al usuario notificando que la transacción solicitada no se completó a través de, al menos, dos canales.

Artículo 24. Notificación de transacciones y operaciones inusuales, irregulares o sospechosas.- La entidad deberá contar con información del número y monto de las transacciones realizadas por medio de canales electrónicos por usuario y tipo de producto, monitoreando además el cumplimiento de los límites y otras medidas prudenciales que se hayan establecido, dependiendo del producto o servicio, e identificando en tiempo real, posibles operaciones inusuales, irregulares o sospechosas de acuerdo con el perfil del usuario y los hábitos de uso de sus productos y servicios financieros, generando las alertas correspondientes sobre tales operaciones.

Las entidades deben notificar en forma inmediata a los usuarios las alertas asociadas a las operaciones realizadas a través de los canales electrónicos, que se desvíen de su perfil transaccional, de manera oportuna y de forma automática, a través de los medios que la entidad estime conveniente.

La notificación o el mensaje enviado deberá describir, como mínimo, fecha y hora de la transacción, monto de la operación, número de referencia de la transacción, nombre y número de teléfono de la entidad, canal utilizado, tipo de producto y de operación.

El monitoreo de las transacciones al que hace referencia el presente artículo deberá ser efectuado por la entidad mediante herramientas informáticas robustas y especializadas en prevención de fraude.

Artículo 25. Reclamos del usuario.- Las entidades deberán contar con un procedimiento establecido y actualizado que les permita atender los reclamos verbales y/o escritos por el uso de canales electrónicos.

Artículo 26. Medios de notificación de reclamos, bloqueos, suspensiones y posibles fraudes.- La entidad establecerá mecanismos y procedimientos adecuados que operen las veinticuatro horas del día, todos los días del año, para atender bloqueos, suspensiones, posibles fraudes y reclamos de los socios, clientes y usuarios sobre sus transacciones, especificando el medio oficial de recepción de los mismos. Se incorporará un protocolo de bloqueo inmediato que será activado una vez que el usuario reporte el extravío o robo del dispositivo o una transacción fraudulenta a través de los canales oficiales, por lo que la entidad deberá:

1. Proceder al bloqueo preventivo, inmediato y temporal de todos o aquellos productos solicitados de manera expresa por el socio, cliente o usuario; tales como, cuentas y canales de acceso del usuario, tarjetas, token digital, etc; y,
2. Confirmar al usuario, en el mismo acto del reclamo, la realización del bloqueo y proporcionar un número de caso o comprobante de la gestión.

Artículo 27. Campañas de educación.- Las entidades deberán informar a sus usuarios, mediante campañas educativas, sobre el funcionamiento de los canales electrónicos que pongan al alcance de estos, a fin de prevenir actos que pudieran derivar en operaciones irregulares o ilegales que afecten a los usuarios o a las propias entidades.

Artículo 28. Comunicación por medios oficiales.- Las entidades deberán informar a sus usuarios los medios oficiales a través de los cuales comunicarán el correcto uso de los productos o servicios que ofrecen.

Artículo 29. Canal de notificación de emergencia.- Las entidades deberán habilitar un canal de comunicación específico para reportar fraudes o cualquier emergencia bancaria. Este canal, que deberá estar claramente identificado en la página web principal y en la aplicación móvil, operará de manera ininterrumpida las 24 horas del día, los 365 días del año, y garantizará la confidencialidad de la información recibida y la entrega inmediata de un comprobante o número de seguimiento de la gestión al denunciante. Para la atención de transacciones no reconocidas, el canal incorporará los siguientes mecanismos:

1. **Botón de Pánico (*Kill Switch*):** Una función prominente en la aplicación móvil (App) y sitio Web que permita al usuario congelar todas sus credenciales y cuentas con un solo toque en caso de sospecha.
2. **Línea de Emergencia:** Un canal telefónico o chat humano 24/7 dedicado a fraudes.

Artículo 30. Reporte de operaciones y transacciones fraudulentas o no reconocidas.- Las entidades deberán asegurar que los IVR, o cualquier otro medio de comunicación facilitado por la entidad, permitan al usuario acceder a opciones para reportar, de forma expedita, las presuntas transacciones u operaciones fraudulentas o no reconocidas y obtener asistencia inmediata para su reclamo, para lo cual deberán establecer procesos específicos con personal debidamente capacitado que brinde atención oportuna a sus usuarios.

Artículo 31. Devolución de valores.- Las entidades deberán contar con un procedimiento documentado para la atención, investigación y resolución de reclamos relacionados con operaciones fraudulentas, no autorizadas o no reconocidas realizadas a través de canales electrónicos, en coordinación con la normativa aplicable sobre atención de reclamos de usuarios financieros. Dicho procedimiento deberá prever, al menos, recepción del reclamo, bloqueo preventivo cuando corresponda, registro de evidencias, análisis técnico y transaccional, determinación de la atribuibilidad del evento, comunicación motivada al usuario y mecanismos de impugnación o revisión conforme a la normativa aplicable. Cuando, como resultado del análisis efectuado por la entidad, se determine que la operación no autorizada o no reconocida no es atribuible al usuario y se encuentra asociada a fallas, vulneraciones o insuficiencias de los controles del canal electrónico o de los servicios provistos por la entidad o por terceros contratados por esta, la entidad deberá reintegrar, compensar o revertir los montos comprometidos, sin cobro de comisiones o recargos adicionales para el usuario. La entidad deberá mantener a

disposición de la Superintendencia de Economía Popular y Solidaria los reportes, estadísticas, evidencias y análisis de causa relacionados con estos eventos, incluyendo el número de denuncias presentadas por socios en los últimos noventa (90) días y las acciones adoptadas para mitigar riesgos de fraude, *phishing* u otras amenazas.

Artículo 32. Cobertura de pérdidas.- Las entidades, con la finalidad de gestionar riesgos originados en incidentes relacionados con vulneraciones a la seguridad de la información asociada con sus canales electrónicos, deberán contratar pólizas de seguros que les permitan cubrir las pérdidas económicas que se deriven de la materialización de estos eventos, o contar con otros mecanismos que en el contexto de la administración de estos riesgos mitiguen su impacto.

Artículo 33. Seguridad en la sesión del usuario.- Respecto de la sesión del usuario, las entidades deberán garantizar lo siguiente:

1. Finalizar la sesión en forma automática en los siguientes casos:
 - a. Cuando existan más de dos (2) minutos de inactividad en canales electrónicos y cinco (5) minutos para banca de empresas;
 - b. Cuando el período de inactividad alcance como máximo los treinta segundos en las operaciones realizadas mediante cajeros automáticos, quioscos o puntos de venta; y,
 - c. Cuando se detecten sesiones simultáneas, se deberá comunicar el hecho al usuario titular del servicio.
2. Comunicar a sus usuarios que, cuando accedan desde el sitio web de la entidad a enlaces de páginas web de terceros, la seguridad de dichos sitios no depende ni es responsabilidad de la entidad.

SECCIÓN V DE LOS RESPALDOS Y AUDITORÍA

Artículo 34. Inventario de activos de información críticos.- Las entidades deberán mantener actualizado el inventario de activos de información críticos e identificar los datos asociados a los mismos. Para la elaboración, actualización y gestión de dicho inventario, las entidades tomarán en cuenta el estándar ISO/IEC 27001 o el estándar equivalente que se encuentre vigente.

Artículo 35. Auditoría de seguridad.- Las entidades deberán establecer y ejecutar procedimientos de auditoría de seguridad en sus canales electrónicos, por lo menos, una vez al año.

Artículo 36. Plan anual de trabajo.- La unidad de auditoría interna de la entidad debe considerar en su plan anual de trabajo la evaluación del cumplimiento de las disposiciones de la presente norma.

Artículo 37. Registro y seguimiento de operaciones.- Los sistemas utilizados en los canales electrónicos de las entidades deberán generar archivos que permitan respaldar el

detalle de los antecedentes de cada operación, de tal forma que estén disponibles para procesos de certificación o auditoría.

Deberán mantener los archivos contables y sus respaldos en físico por el plazo de diez años contados a partir de la fecha de conclusión de la operación y por quince años en formato digital. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

Asimismo, deberán conservar durante al menos seis meses los registros de las comunicaciones realizadas por los usuarios a los centros de atención no presenciales. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales.

Artículo 38. Protección de datos en entornos de pruebas y desarrollo.- Las entidades no podrán utilizar datos reales de usuarios (incluyendo información personal, credenciales, números de cuenta, o datos transaccionales) en entornos de desarrollo, pruebas de software, control de calidad, o capacitación, a menos que dichos datos hayan sido previamente anonimizados o desensibilizados mediante técnicas que impidan la reidentificación de las personas. Los entornos de pruebas deberán:

1. Estar aislados de la infraestructura de producción, con controles de acceso independientes y segregación de redes;
2. Utilizar credenciales ficticias y datos sintéticos que no correspondan a usuarios reales;
3. Ser sometidos a las mismas medidas de seguridad de la información que los entornos de producción, en lo que resulte aplicable;
4. Ser desincorporados o limpiados de datos sensibles una vez concluida su finalidad. La auditoría interna verificará semestralmente el cumplimiento de esta disposición.

SECCIÓN VI DE LAS RESPONSABILIDADES

Artículo 39. Responsabilidades de las cooperativas de ahorro y crédito de los segmentos 1, 2 y 3, cajas centrales y asociaciones mutualistas de ahorro y crédito para la vivienda.- Las entidades señaladas en el presente artículo serán responsables de implementar, mantener y fortalecer los controles de seguridad de la información, ciberseguridad y gestión de riesgos asociados a las transferencias electrónicas y a los canales electrónicos utilizados para la prestación de servicios financieros.

Para dicho efecto, deberán cumplir al menos con las siguientes responsabilidades:

1. Implementar controles técnicos, operativos y de atención al usuario que permitan prevenir, detectar y mitigar los riesgos de fraude electrónico, phishing, suplantación de identidad y otras amenazas cibernéticas asociadas al uso de canales electrónicos, incluso cuando el evento se origine fuera de la infraestructura tecnológica de la entidad;

2. Implementar mecanismos de autenticación fuerte basados en riesgo, que incluyan al menos múltiples factores de autenticación, validaciones asociadas al dispositivo utilizado por el cliente, monitoreo transaccional y alertas en tiempo real sobre operaciones realizadas, así como mecanismos de notificación y canales de reporte o denuncia de fraude disponibles de forma permanente, que permitan una reacción oportuna ante eventos de seguridad;
3. El Consejo de Administración aprobará las políticas, procesos y procedimientos relacionados con la seguridad en las transferencias electrónicas y en los canales electrónicos, los cuales deberán contemplar, al menos, las responsabilidades internas de la entidad y las responsabilidades de los proveedores o terceros que participen en la prestación de dichos servicios;
4. El comité de administración integral de riesgos propondrá al consejo de administración las políticas, procesos y procedimientos relacionados con la gestión de los riesgos asociados a la seguridad en las transferencias electrónicas y en los canales electrónicos, así como sus respectivas actualizaciones;
5. El representante legal será responsable de implementar y asegurar el cumplimiento de las políticas, procesos y procedimientos aprobados por el consejo de administración en materia de seguridad en las transferencias electrónicas y gestión de riesgos asociados;
6. La unidad de tecnología de la información o el responsable de tecnología, conjuntamente con el responsable de seguridad de la información, cuando corresponda, elaborará y presentará al comité de administración integral de riesgos las políticas, procesos y procedimientos relacionados con la gestión de los riesgos de seguridad en las transferencias electrónicas y canales electrónicos, así como sus actualizaciones, considerando el análisis de riesgos institucional, estándares internacionales y buenas prácticas en materia de seguridad de la información y ciberseguridad; y,
7. Auditoría interna verificará periódicamente la efectividad de los controles y medidas de seguridad implementadas para las transferencias electrónicas y los canales electrónicos, y emitirá recomendaciones para la adopción de acciones correctivas cuando corresponda. Asimismo, deberá custodiar los informes de pruebas de vulnerabilidad, pruebas de penetración u otras evaluaciones de seguridad realizadas, y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria cuando esta lo requiera.

Artículo 40. Responsabilidades de las cooperativas de ahorro y crédito de los segmentos 4 y 5.- Las entidades descritas en el presente artículo tendrán las siguientes responsabilidades:

1. El Consejo de Administración aprobará las políticas, procesos y procedimientos referentes a la seguridad en las transferencias electrónicas, definiendo específicamente las responsabilidades internas y del proveedor;
2. El representante legal deberá proponer al consejo de administración las políticas, procesos y procedimientos referentes a la seguridad en las transacciones electrónicas y su gestión de riesgos, recomendando su aprobación; y,
3. El Consejo de Vigilancia verificará la efectividad de las medidas de seguridad en las transacciones electrónicas y recomendará medidas correctivas.

Artículo 41. Responsabilidades de las organizaciones y compañías de servicios auxiliares del sector financiero popular y solidario.- Las organizaciones y compañías de servicios auxiliares que participen directa o indirectamente en la operación, administración, procesamiento, soporte o prestación de servicios financieros a través de canales electrónicos serán responsables, dentro del ámbito de las actividades y servicios que presten, de implementar, mantener y fortalecer los controles de seguridad de la información, ciberseguridad, continuidad operativa y gestión de riesgos tecnológicos previstos en la presente norma.

El alcance y nivel de aplicación de dichas responsabilidades serán proporcionales a la naturaleza, volumen, complejidad y criticidad de los servicios prestados, así como a los riesgos que su interrupción, vulneración o funcionamiento inadecuado puedan generar para las entidades financieras, sus socios, clientes y usuarios.

Para el efecto, deberán cumplir, al menos, con las siguientes responsabilidades:

1. El órgano de administración, directorio o máxima instancia de gobierno que corresponda deberá aprobar las políticas, procesos y procedimientos relacionados con seguridad de la información, ciberseguridad, gestión de riesgos tecnológicos, continuidad operativa, protección de datos personales y gestión de incidentes aplicables a los servicios prestados;
2. El representante legal será responsable de implementar y asegurar el cumplimiento de las políticas, procesos, procedimientos y controles aprobados, así como de asignar los recursos humanos, tecnológicos y financieros necesarios para su ejecución;
3. Contar con una unidad, responsable o función encargada de la tecnología, seguridad de la información y ciberseguridad, de acuerdo con la naturaleza, tamaño, complejidad y criticidad de los servicios prestados, procurando una adecuada segregación de funciones;
4. Implementar controles técnicos y operativos destinados a prevenir, detectar, contener, responder y recuperarse de incidentes de seguridad, ataques cibernéticos, fraude electrónico, accesos no autorizados, pérdida o alteración de información e interrupciones de los servicios;
5. Implementar, según corresponda, controles de acceso, autenticación, cifrado, monitoreo, trazabilidad, gestión de vulnerabilidades, actualización de componentes tecnológicos, desarrollo seguro, respaldo de información y conservación de registros;
6. Contar con planes de continuidad operativa, contingencia y recuperación ante desastres, debidamente documentados, actualizados y sometidos a pruebas periódicas, especialmente respecto de los servicios, procesos e infraestructuras considerados críticos;
7. Comunicar oportunamente a las entidades contratantes y a la Superintendencia de Economía Popular y Solidaria los incidentes de seguridad o continuidad que puedan afectar la confidencialidad, integridad o disponibilidad de la información, la prestación de servicios financieros o los derechos de los usuarios, de

- conformidad con los plazos, mecanismos y condiciones establecidos en la normativa aplicable;
8. Proteger la confidencialidad, integridad, disponibilidad, reserva y sigilo de la información a la que tengan acceso, y tratar los datos personales de conformidad con la Ley Orgánica de Protección de Datos Personales, según el rol que les corresponda dentro de cada tratamiento;
 9. Realizar procesos de debida diligencia y control respecto de proveedores, subcontratistas y terceros que intervengan en la prestación de los servicios, sin que la contratación o subcontratación los exonere de las responsabilidades establecidas en la presente norma;
 10. Mantener registros, evidencias, bitácoras, informes técnicos y demás documentación que permitan verificar la trazabilidad de las operaciones, la aplicación de controles, la gestión de incidentes y el cumplimiento de las obligaciones previstas en esta norma;
 11. Permitir y facilitar la realización de auditorías, evaluaciones, pruebas de seguridad e inspecciones por parte de la Superintendencia de Economía Popular y Solidaria y de las entidades contratantes, dentro del ámbito de sus respectivas competencias y relaciones contractuales;
 12. Incorporar en los contratos, convenios, acuerdos de nivel de servicio y anexos técnicos las responsabilidades de las partes, niveles mínimos de disponibilidad, continuidad, seguridad, confidencialidad, protección de datos personales, reporte de incidentes, auditoría, subcontratación, devolución o eliminación de información y mecanismos de terminación del servicio; y,
 13. Disponer que la auditoría interna, o la instancia independiente que haga sus veces, verifique periódicamente la efectividad de los controles implementados y recomiende las acciones correctivas que correspondan.

Cuando las organizaciones o compañías de servicios auxiliares presten servicios críticos, transaccionales, de procesamiento de operaciones, almacenamiento o alojamiento de información, computación en la nube, autenticación, ciberseguridad u operación de canales electrónicos, deberán aplicar controles reforzados y mantener mecanismos permanentes de monitoreo, continuidad, respuesta a incidentes y evaluación independiente.

El cumplimiento de las responsabilidades previstas en este artículo no exime a las entidades financieras contratantes de las obligaciones que les corresponden conforme a la presente norma. De igual manera, las organizaciones y compañías de servicios auxiliares serán directamente responsables por los actos u omisiones que se produzcan dentro del ámbito de los servicios a su cargo.

Lo dispuesto en este artículo se aplicará sin perjuicio de las obligaciones establecidas en la normativa específica que regula o regule a las organizaciones y compañías de servicios auxiliares del sector financiero popular y solidario.

SECCIÓN VII

DE LA PUBLICACIÓN Y ACTUALIZACIÓN DE APLICACIONES Y CANALES ELECTRÓNICOS

Artículo 42. Requisitos previos a la publicación de aplicaciones y canales electrónicos.- Las entidades no podrán poner a disposición de los usuarios, en tiendas de aplicaciones oficiales o mediante cualquier otro medio de distribución, una aplicación móvil, actualización de esta, o cualquier nuevo canal electrónico (incluyendo sitios web transaccionales, APIs, o versiones significativas de software), sin que previamente se hayan completado y aprobado las siguientes etapas mínimas de control interno:

1. Desarrollo seguro conforme a estándares reconocidos (OWASP, NIST, ISO 27001), incluyendo análisis estático y dinámico de código, revisión de dependencias y bibliotecas de terceros;
2. Pruebas de penetración y evaluación de vulnerabilidades específicas para el canal o aplicación, realizadas por personal interno independiente del área de desarrollo o por un tercero especializado;
3. Revisión y validación de los controles de seguridad de la información, autenticación, autorización, cifrado, manejo de sesiones, y prevención de fraudes por parte de la unidad de tecnología o seguridad de la información;
4. Aprobación formal del comité de administración integral de riesgos o la instancia que haga sus veces, documentando la verificación del cumplimiento de la presente norma y de las políticas internas de seguridad; y,
5. Registro de la versión, fecha de publicación, y evidencias de las pruebas realizadas, las cuales deberán conservarse por un plazo mínimo de cinco (5) años.

DISPOSICIONES GENERALES

PRIMERA.- En la aplicación de la presente norma, todo tratamiento de datos personales efectuado por las entidades deberá sujetarse a la Ley Orgánica de Protección de Datos Personales y demás normativa aplicable.

Las entidades deben garantizar que dichos tratamientos respondan a finalidades determinadas, explícitas y legítimas, relacionadas con la seguridad de los canales electrónicos, la prevención y detección del fraude, la gestión de riesgos y el cumplimiento de obligaciones legales; y que sean adecuados, pertinentes, necesarios y proporcionales a tales finalidades. Además deben generar planes y programas que les permitan dar cumplimiento con lo dispuesto en la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás normativa vigente emitida por la Autoridad de Control y Vigilancia de Protección de Datos Personales.

Los datos personales no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su tratamiento, ni podrán recopilarse o conservarse datos excesivos respecto de la finalidad perseguida, sin perjuicio de los plazos de conservación previstos en la legislación aplicable.

SEGUNDA.- La implementación, habilitación o utilización de canales electrónicos no requerirá autorización expresa de la Superintendencia, sin perjuicio del cumplimiento de

las disposiciones previstas en la presente norma y de los requisitos técnicos, operativos, de seguridad, gestión de riesgos y control interno aplicables

TERCERA.- Cuando se usen terminales electrónicos ajenos a la red de la entidad financiera, esta deberá asegurarse de que dichos terminales electrónicos cuenten con todas las seguridades requeridas en la presente norma.

CUARTA.- Las entidades que presten servicios por medio de canales electrónicos a través de otras entidades del sistema financiero nacional, compañías u organizaciones de servicios auxiliares del sistema financiero deberán celebrar los respectivos contratos, de conformidad con lo dispuesto en la presente norma.

En dichos contratos deberán establecerse de manera expresa las responsabilidades de la entidad contratante y de la entidad financiera, compañía u organización de servicios auxiliares contratada, particularmente en materia de seguridad de la información, ciberseguridad, continuidad operativa, confidencialidad, protección de datos personales, gestión y reporte de incidentes, niveles de servicio, auditoría y mecanismos de terminación del servicio.

QUINTA.- Las entidades, previa autorización de la Superintendencia de Economía Popular y Solidaria, podrán celebrar convenios de asociación para ofrecer sus servicios a través de transferencias electrónicas, garantizando que las entidades participantes cumplan con lo dispuesto en esta norma.

SEXTA.- Los casos de duda en la aplicación de la presente Norma serán resueltos por la Superintendencia de Economía Popular y Solidaria.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las entidades controladas deberán adecuar sus políticas, procesos, procedimientos, contratos, canales electrónicos, aplicaciones, infraestructura tecnológica, mecanismos de autenticación, monitoreo, atención de reclamos, reportes y demás controles previstos en la presente norma, dentro de los plazos máximos establecidos a continuación, contados a partir de la entrada en vigencia de esta resolución:

Entidad	Plazo máximo de adecuación	Alcance mínimo durante el período de transición
Cooperativas de ahorro y crédito de los segmentos 1, 2 y 3; cajas centrales; y, asociaciones mutualistas de ahorro y crédito para la vivienda	Doce (12) meses	Implementación integral de las obligaciones previstas en la presente norma, de acuerdo con la criticidad de los canales electrónicos y el perfil de riesgo institucional.

Cooperativas de ahorro y crédito de los segmentos 4 y 5	Veinticuatro (24) meses	Implementación progresiva y proporcional, considerando tamaño, complejidad, nivel de exposición tecnológica y servicios efectivamente ofrecidos por canales electrónicos.
---	-------------------------	---

SEGUNDA.- Durante los plazos de adecuación señalados en la disposición transitoria primera, las entidades deberán aplicar la presente norma de forma progresiva, conforme a su planificación interna y al nivel de riesgo de los canales electrónicos que administren. Las obligaciones de seguridad, monitoreo, bloqueo preventivo, atención de reclamos, notificación de incidentes y protección del usuario deberán priorizarse respecto de los canales, servicios y operaciones de mayor criticidad o exposición al riesgo tecnológico, operacional o de fraude.

TERCERA.- Hasta que venza el plazo de adecuación aplicable a cada tipo de entidad, se mantendrán vigentes para dicha entidad las disposiciones de la Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 y sus reformas, únicamente en aquello que resulte necesario para asegurar la continuidad de los controles de seguridad en transferencias electrónicas y siempre que no se opongan a la presente norma. En caso de contradicción, prevalecerán las disposiciones de esta resolución.

CUARTA.- Las entidades deberán aprobar un plan de adecuación que contenga, al menos: diagnóstico de brechas frente a la presente norma; actividades, responsables y cronograma de implementación; identificación de canales y servicios críticos; priorización de controles por nivel de riesgo; necesidades contractuales con proveedores tecnológicos; mecanismos de seguimiento; y evidencias de cumplimiento. El plan deberá estar a disposición de la Superintendencia de Economía Popular y Solidaria cuando esta lo requiera.

QUINTA.- Los canales electrónicos, aplicaciones, servicios digitales, terminales, convenios o contratos que se encuentren operativos a la fecha de entrada en vigor de la presente norma podrán continuar funcionando durante el período de adecuación aplicable, siempre que la entidad mantenga controles mínimos de seguridad, continuidad, monitoreo, atención de incidentes y protección del usuario. Las nuevas aplicaciones, canales electrónicos o actualizaciones significativas que se implementen con posterioridad a la entrada en vigor de la presente norma deberán observar los requisitos previstos en esta resolución, en especial los establecidos para la publicación y actualización de aplicaciones y canales electrónicos.

SEXTA.- Las entidades deberán revisar y, de ser necesario, adecuar los contratos, convenios, acuerdos de nivel de servicio, anexos técnicos y demás instrumentos suscritos con proveedores tecnológicos, entidades financieras, compañías u organizaciones de servicios auxiliares del sistema financiero u otros terceros que participen en la prestación de servicios por canales electrónicos, a fin de incorporar las responsabilidades, controles,

niveles de servicio, medidas de seguridad, continuidad, confidencialidad, auditoría, reporte de incidentes y demás obligaciones previstas en la presente norma, dentro del plazo de adecuación aplicable.

SÉPTIMA.- La Superintendencia de Economía Popular y Solidaria podrá requerir a las entidades, en cualquier momento durante el período de transición, información, evidencias, reportes de avance, planes de acción o medidas correctivas relacionadas con el cumplimiento progresivo de esta norma, de acuerdo con sus atribuciones de control y supervisión.

OCTAVA.- Las organizaciones y compañías de servicios auxiliares del sector financiero popular y solidario estarán sujetas a las disposiciones de la presente resolución que les resulten aplicables, de acuerdo con la naturaleza, alcance y características de los servicios que presten a las entidades financieras bajo control de la Superintendencia de Economía Popular y Solidaria, y mientras no conste una normativa específica aplicable a las mismas.

NOVENA.- Los procedimientos administrativos sancionadores iniciados con anterioridad a la entrada en vigor de la presente resolución continuarán sustanciándose conforme al régimen procedimental aplicable. Las infracciones y sanciones se registrarán por las disposiciones vigentes al momento de los hechos.

DISPOSICIÓN DEROGATORIA ÚNICA.- Deróguese la Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 y sus reformas una vez que venzan los plazos de adecuación previstos en la disposición transitoria primera de la presente resolución, según corresponda a cada sujeto obligado.

Hasta el vencimiento de dichos plazos, la Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 y sus reformas continuará siendo aplicable durante el respectivo período de adecuación, únicamente en aquello que resulte necesario para garantizar la continuidad de los controles de seguridad y siempre que sus disposiciones no se opongan a la presente resolución. En caso de contradicción, prevalecerán las disposiciones de esta última.

DISPOSICIÓN FINAL.- La presente norma entrará en vigencia a partir de su suscripción, sin perjuicio de los plazos de adecuación previstos en sus disposiciones transitorias, y de la respectiva publicación en el Registro Oficial.

Publíquese en la página web de la Superintendencia de Economía Popular y Solidaria.

COMUNÍQUESE Y PUBLÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los 28 días de septiembre de 2026.



FREDDY ALFONSO MONGE MUÑOZ
INTENDENTE GENERAL TÉCNICO



Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

JL/FA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"

El Registro Oficial no se responsabiliza por los errores ortográficos, gramaticales, de fondo y/o de forma que contengan los documentos publicados, dichos documentos remitidos por las diferentes instituciones para su publicación, son transcritos fielmente a sus originales, los mismos que se encuentran archivados y son nuestro respaldo.