Diario Oficial
LA GACETA
Costa Rica
145 años



Benemérita
Imprenta Nacional
Costa Rica

# ALCANCE Nº 166 A LA GACETA Nº 159

Año CXLV | San José, Costa Rica, jueves 31 de agosto del 2023 | 68 páginas

# PODER EJECUTIVO

## DECRETOS

# REGLAMENTOS

## JUNTA DE PROTECCIÓN SOCIAL

Imprenta Nacional
La Uruca, San José, C. R.

# PODER EJECUTIVO

## DECRETOS

### Nº 44196-MSP-MICITT

**EL PRESIDENTE DE LA REPÚBLICA,**
**EL MINISTRO DE SEGURIDAD PÚBLICA Y LA MINISTRA DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES**

En el ejercicio de las atribuciones que les confieren los artículos 11, 24, 33, 34, 46, 121 inciso 14) subinciso c), 140 y 146 de la Constitución Política emitida en fecha 07 de noviembre de 1949 y publicada en la Colección de Leyes y Decretos del Año: 1949, Semestre: 2, Tomo: 2, Página: 724 y sus reformas; en el Anexo 13 de la Ley N° 8622, "Tratado de Libre Comercio República Dominicana - Centroamérica - Estados Unidos (TLC)" emitido en fecha 21 de noviembre de 2007 y publicado en el Alcance N° 40 al Diario Oficial La Gaceta N° 246 de fecha 21 de diciembre de 2007, en el "Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) aprobado mediante la Ley N° 9452 "Aprobación de la Adhesión al Convenio sobre la Ciberdelincuencia", emitida en fecha 26 de mayo de 2017 y publicada en el Alcance N°161 al Diario Oficial La Gaceta N°125 de fecha 03 de julio de 2017, en los artículos 4, 8, 10, 11, 12, 13, 15, 16, 25 inciso 1), 27 inciso 1), 28 inciso 2) acápite b), 113, 120, 121, 133, 136 inciso e), 240, y 307 inciso 2) de la Ley Nº 6227, "Ley General de la Administración Pública", emitida en fecha 02 de mayo de 1978 y publicada en la Colección de Leyes y Decretos del Año: 1978, Semestre: 1, Tomo: 4, Página: 1403 y sus reformas; los artículos 11, 20 inciso e) y 21 de la Ley Nº7169, "Ley de Promoción del Desarrollo Científico y Tecnológico" emitida en fecha 26 de junio de 1990 y publicada en el Alcance N°23 al Diario Oficial La Gaceta N°144 de fecha 01 de agosto de 1990 y sus reformas, en los artículos 1, 2 incisos d) e) y f), 3 incisos c), d), f), i), j), 4, 6 incisos 7), 12), 16), 19), 23), y 30), 7, 8, 10, 41, 42, 45, 49 incisos 1, 2 y 3 de la Ley N° 8642, "Ley General de Telecomunicaciones" (LGT), emitida en fecha 04 de junio de 2008 y publicada en el Diario Oficial La Gaceta N° 125 de fecha 30 de junio de 2008 y sus reformas, en los artículos 1, 2, 3, 38, 39 y 40 de la Ley N° 8660, "Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones", emitida en fecha 08 de agosto de 2008 y

publicada en el Alcance N° 31, al Diario Oficial La Gaceta N° 156 de fecha 13 de agosto de 2008 y sus reformas; el artículo 1 de la Ley N°5482, “Ley Orgánica del Ministerio de Seguridad”, emitida el 24 de diciembre de 1973 y publicada en la Colección de Leyes y Decretos del año 1973, Semestre 2, Tomo 4, página 1858 y sus reformas, los artículos 13 y 14 de la Ley N° 7410 “Ley General de Policía”, emitida el 26 de mayo de 1994, y publicada en el Alcance N°16 al Diario Oficial La Gaceta N°103, de fecha 30 de mayo de 1994 y sus reformas, el artículo 1 de la Ley N° 8220, “Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos” emitida el 04 de marzo de 2002 y publicada en el Alcance N°22 al Diario Oficial La Gaceta N°22 de fecha 11 de marzo de 2002 y sus reformas; los artículos 4 y 25 de la Ley N°8488, “Ley Nacional de Emergencias y Prevención del Riesgo” emitida el 22 de noviembre de 2005 y publicada en el Diario Oficial La Gaceta N° 8 de fecha 11 de enero de 2006 y sus reformas, el Decreto Ejecutivo N° 37052-MICIT "Crea Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR" emitido el 09 de marzo de 2012, y publicado en el Diario Oficial La Gaceta N°72 de fecha 13 de abril de 2012; el Decreto Ejecutivo N° 40546-RREE “Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001)” emitido el 03 de julio de 2017 y publicado en el Diario Oficial La Gaceta N° 156 de fecha 18 de agosto de 2017; el Decreto Ejecutivo N°43542-MP-MICITT,“Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información”, emitido el 08 de mayo de 2022 y publicado en el Alcance N°94 al Diario Oficial La Gaceta N°86 de fecha 11 de mayo de 2005; el artículo 2 del Decreto Ejecutivo Nº 44010-MINAET denominado “Plan Nacional de Atribución de Frecuencias (PNAF)”, emitido en fecha 16 de marzo de 2023, y publicado en el Alcance N°99 al Diario Oficial La Gaceta Nº 95 de fecha 30 de mayo 2023, en el artículo 2 del Decreto Ejecutivo N° 38767-MP-MTSS-MJP**,** denominado “Reglamento al artículo 375 del Código de Trabajo” emitido el 18 de diciembre de 2014, y publicado en el Diario Oficial La Gaceta N°20 de 29 de enero de 2015; en el Plan Nacional de Desarrollo de las Telecomunicaciones 2022-20217 “Costa Rica: Hacia la disrupción digital inclusiva” y el Informe técnico Nº MICITT-

DGDCFD-INF-007-2023 de fecha 25 de agosto de 2023 denominado “Ciberseguridad en Redes 5G” emitido por la Dirección de Gobernanza Digital y Certificadores de Firma Digital, del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, y ;

**CONSIDERANDO:**

I. Que, el artículo 24 de la Constitución Política garantiza los derechos fundamentales a la intimidad, la privacidad y el secreto de las comunicaciones, y el derecho de autodeterminación informativa los cuales se sustentan en la dignidad de la persona y la autodeterminación consciente y responsable de la propia vida.

II. Que, por lo anterior se afirma que la dignidad *es inherente al ser humano, y es el mínimo jurídico que se le debe asegurar a la persona con el objeto de que se respete su condición de tal y un mínimo de calidad de vida humana. En el respeto de los derechos derivados del artículo 24 se manifiesta el respeto a la dignidad humana.”* (Procuraduría General de la República, Opinión Jurídica OJ-103-2010, del 13 de diciembre de 2010).

III. Que, ese sentido, como derivado de la dignidad e intimidad humanas, el tratamiento de los datos personales se encuentra dispuesto en un régimen jurídico especial que garantiza un trato adecuado de los mismos, por ello la Procuraduría General de la República en su Dictamen N° C-064-2022 de fecha 22 de marzo de 2022 manifestó:

> *“Por ejemplo, se prohíbe el tratamiento por parte de terceros, de aquellos datos considerados sensibles o personales, en cuyo caso, se consideran confidenciales, además, se protegen los datos personales de acceso restringido, los cuales, aún y cuando consten en registros de acceso al público, no pueden ser de acceso irrestricto, de allí que, su tratamiento está permitido sólo para el titular de la Administración Pública interesada, cuando persiga fines públicos, o bien, se cuente con el consentimiento expreso del titular.”*

IV. Que, el artículo 34 de la Constitución Política dispone el principio de seguridad jurídica para la debida protección de los derechos subjetivos y patrimoniales adquiridos o de situaciones jurídicas consolidadas. Se procura, además, que los administrados conozcan de previo a qué atenerse frente al ejercicio de la función administrativa y recibir de la administración pública un comportamiento leal, ajustado a parámetros de certidumbre y predictibilidad, para evitar situaciones objetivamente confusas, o situaciones jurídicas no conformes con el ordenamiento jurídico.

V. Que, esta garantía de seguridad al individuo *"por la cual, tiene la certeza de que su situación jurídica no será modificada más que por procedimientos regulares, establecidos previamente, es decir, representa la garantía de la aplicación objetiva de la ley, en tanto los individuos saben en cada momento cuáles son sus derechos y obligaciones."*. (Sala Constitucional mediante su Resolución N° 2010-03946 de las 14:44 horas de fecha 24 de febrero de 2010).

VI. Que, por su parte el artículo 46 de la Constitución Política reconoce la libertad de empresa, la libre concurrencia en el mercado, así como la protección al conjunto de intereses y derechos de los usuarios finales quienes gozan de *"(…) la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo."*.

VII. Que, mediante la Ley N°9452 se aprobó, en cada una de sus partes, la adhesión al Convenio sobre la Ciberdelincuencia, hecha en Budapest el 23 de noviembre de 2001, siendo un instrumento jurídico fundamental en la lucha contra la ciberdelincuencia, cuyo propósito principal es prevenir, investigar y sancionar los delitos cibernéticos, fortalecer la seguridad de los sistemas de información y fomentar la cooperación internacional en esta materia.

VIII. Que el preámbulo del Convenio sobre la Ciberdelincuencia establece que resulta "(…) necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable; (…)".

IX. Que, por disposición del inciso 14), sub inciso c), del artículo 121 de la Constitución Política el espectro radioeléctrico es un bien demanial constitucional que únicamente puede ser explotado por la administración pública o por particulares, de acuerdo con la ley o mediante concesión especial otorgada por tiempo limitado y con arreglo a las condiciones y estipulaciones que establezca la Asamblea Legislativa.

X. Qué, el constituyente originario ha dispuesto que el uso y explotación del espectro radioeléctrico o electromagnético puede darse en un régimen de competencia y libre concurrencia, tanto por la administración pública o por particulares conforme a la constitución económica siendo *"el deseo del Constituyente que los particulares participen de la explotación de este bien, siempre y cuando, se cumplan con las condiciones estipuladas en la propia Norma Fundamental.". (*Sala Constitucional, mediante Resolución N.º 04569 – 2008, del 26 de marzo del 2008.).

XI. Que, debido a lo anterior, conforme lo dispone el artículo 140 inciso 8 de la Constitución Política, corresponde al Presidente de la República y a los Ministerios de Seguridad Pública y de Ciencia, Innovación, Tecnología y Telecomunicaciones, vigilar el buen funcionamiento de los servicios de telecomunicaciones, en resguardo de bienes jurídicos tutelados superiores como lo son la dignidad humana, la intimidad y la seguridad.

XII. Que, los principios constitucionales del buen funcionamiento y continuidad del, servicio público contenidos en el artículo 4 de la Ley General de la Administración Pública, Ley Nº 6227, expresan que la conducta administrativa en relación con el servicio público debe estar dirigida a asegurar la continuidad, eficiencia y adaptación al cambio, asimismo en la ***"****igualdad en el trato de los destinatarios, usuarios o beneficiarios".*

XIII. Que, el artículo 1 de la Ley General de Telecomunicaciones, Ley N° 8642, establece que estarán sometidas al ordenamiento sectorial y a la jurisdicción costarricense, las personas, físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que operen redes o presten servicios de telecomunicaciones que se originen, terminen o transiten por el territorio nacional.

XIV. Que, el artículo 2, incisos d), e), y f) de la Ley General de Telecomunicaciones, Ley N° 8642, establece los objetivos sectoriales con enfoque de protección de los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios, así como garantizar la privacidad y confidencialidad en las comunicaciones; la promoción de la competencia efectiva en el mercado de las telecomunicaciones; así como la promoción del desarrollo y uso de los servicios de telecomunicaciones dentro del marco de la Sociedad de la Información y el Conocimiento.

XV. Que, el artículo 3 incisos c), d), f), i), j), de la misma Ley General de Telecomunicaciones, Ley N° 8642, establece que nuestro ordenamiento jurídico sectorial se basa en principios rectores como lo son el beneficio al usuario final de los servicios de telecomunicaciones, la transparencia, la optimización del recurso escaso, privacidad de la información, competencia efectiva, principios orientadores de la función administrativa del Ente Rector de las Telecomunicaciones y de la actividad del Poder Ejecutivo, que derivan de las mismas normas constitucionales referidas ut supra.

XVI. Que, el artículo 4 de la Ley General de Telecomunicaciones, Ley N° 8642, establece la especialidad de esta Ley sobre otras normas de carácter general, y, por tanto, su aplicación de manera prioritaria sobre cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en contrario.

XVII. Que, el artículo 6 incisos 7), 12), 16), 19), 23), y 30) de la Ley General de Telecomunicaciones, Ley N° 8642, estipula una serie de definiciones (v.gr. usuario final de telecomunicaciones, red de telecomunicaciones, competencia efectiva, operador, proveedor entre otras), que orientan la aplicación del régimen jurídico sectorial y que además informan el contenido de la normativa sectorial hacia la plena satisfacción del interés público que reviste el eficiente y seguro uso y explotación del espectro radioeléctrico, y de forma particular en el contexto de la presente normativa reglamentaria, en relación con quienes operen redes o presten servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y la protección efectiva que debe darse sobre el régimen jurídico de protección a los derechos de los usuarios finales que comprende la intimidad, la privacidad y secreto de sus comunicaciones y autodeterminación informativa.

XVIII. Que, en concordancia con lo anterior, en los artículos 7, 8 inciso a) y 10 de la Ley General de Telecomunicaciones, Ley N° 8642, se establece que el espectro radioeléctrico es un bien de dominio público y que su planificación, administración y control se llevará a cabo según lo establecido en la Constitución Política, los tratados internacionales, la Ley General de Telecomunicaciones, el Plan Nacional de Desarrollo de las Telecomunicaciones, el Plan Nacional de Atribución de Frecuencias y los demás reglamentos que al efecto se emitan.

XIX. Que, el Título II, Capítulo II denominado Régimen de Protección a la intimidad y derechos de los usuarios finales de la Ley General de Telecomunicaciones, Ley N° 8642, se establece una norma especial que regula el régimen de privacidad y

de protección de los derechos e intereses de los usuarios finales de los servicios de telecomunicaciones, y de forma específica los artículos 41 y 42 de este cuerpo legal disponen la obligación de los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público, de garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios finales, mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias de protección que sean fijadas reglamentariamente por el Poder Ejecutivo.

XX. Que, aunado a lo anterior, para garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los usuarios finales de telecomunicaciones, hay un compromiso legalmente dispuesto para múltiples partes, que se constituye en una relación jurídica triangular conexa, en donde en primer lugar se tiene a los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público quienes tienen la obligación de implementar los sistemas y las medidas técnicas y administrativas necesarias que conlleven la protección de los citados derechos, en segundo lugar, el Poder Ejecutivo debe de disponer reglamentariamente las regulaciones pertinentes con un ámbito de sujeción que comprende a los operadores y proveedores de servicios de telecomunicaciones disponibles al público y, por último, las funciones delegadas a la Superintendencia de Telecomunicaciones de verificar y fiscalizar por el cumplimiento de tales medidas de protección. Todo ello a favor del régimen jurídico de protección a los usuarios finales en el acceso y disfrute de los servicios de telecomunicaciones.

XXI. Que, el artículo 49 incisos, 1, 2 y 3, de la Ley General de Telecomunicaciones, Ley N° 8642, establece como parte de las obligaciones de los operadores y proveedores de servicios de telecomunicaciones el deber de cumplir con las condiciones que establezca su título habilitante, pero además con los reglamentos y las demás disposiciones que se dicten, así como respetar los derechos de los usuarios de telecomunicaciones y atender sus reclamaciones.

XXII. Que, la Ley General de la Administración Pública, Ley Nº6227, en su artículo 14 inciso 1) establece que *"Los principios generales de derecho podrán autorizar implícitamente los actos de la Administración Pública necesarios para el mejor desarrollo de las relaciones especiales creadas entre ella y los particulares por virtud de actos o contratos administrativos de duración.".*

XXIII. Que, la Ley General de la Administración Pública, Ley Nº6227, en su artículo 59 inciso 1) dispone que *"1. La competencia será regulada por ley siempre que contenga la atribución de potestades de imperio."*

XXIV. Que, la misma Ley General de la Administración Pública, Ley Nº6227, en su artículo 113 inciso 3) determina que *"En la apreciación del interés público se tendrá en cuenta, en primer lugar, los valores de seguridad jurídica y justicia para la comunidad y el individuo, a los que no puede en ningún caso anteponerse la mera conveniencia."*.

XXV. Que, mediante el artículo 11 de la Ley de Promoción del Desarrollo Científico y Tecnológico, Ley Nº7169, se define que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) será el rector del Sistema Nacional de Ciencia, Tecnología e Innovación, con funciones orgánicas de articulación y coordinación en los campos de desarrollo científico, tecnológico y de la innovación.

XXVI. Que, en ese sentido el artículo 20 de la Ley de Promoción del Desarrollo Científico y Tecnológico, Ley Nº7169, dispone que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) es el órgano rector en materia de ciencia, innovación, tecnología y telecomunicaciones, particularmente el inciso e) de dicho numeral, le delega *"Promover la creación y el mejoramiento de los instrumentos jurídicos y administrativos necesarios para el desarrollo científico, tecnológico y de la innovación del país".*

XXVII. Que, el artículo 21 de la citada Ley de Promoción del Desarrollo Científico y Tecnológico, Ley Nº7169, define que: “Las competencias del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) serán ejercidas por su ministro, salvo que sean delegadas por él mismo o por disposición del reglamento, siempre que no sean las reservadas al Poder Ejecutivo, según la Constitución Política y los artículos 27 y 28 de la Ley 6227, Ley General de la Administración Pública, de 2 de mayo de 1978.”.

XXVIII. Que, de conformidad con el artículo 1 de la Ley N°5482, “Ley Orgánica del Ministerio de Seguridad Pública”, dicho Ministerio, tiene por función preservar y mantener la soberanía nacional, velar por la seguridad, tranquilidad y el orden público en el país, por lo qué, representa un actor esencial en la prevención de situaciones que pudiesen afectar o impactar el régimen jurídico de protección a los usuarios finales de los servicios de telecomunicaciones, en resguardo de derechos fundamentales como la dignidad, intimidad, seguridad, acceso a la información, la libre comunicación, salud, entre otros.

XXIX. Que en concordancia con lo anterior, el ordinal 1, de la Ley General de Policía, Ley N°7410, establece que el Estado garantizará la seguridad pública, para ello, el Presidente de la República y el Ministro del Ramo, podrán disponer medidas necesarias para garantizar el orden, la defensa y la seguridad del país, así como las que aseguren la tranquilidad y el libre disfrute de las libertades públicas.

XXX. Que, en concordancia, los artículos 13 y 14 de la Ley General de Policía, Ley N°7410, disponen que, la Dirección de Inteligencia y Seguridad Nacional, consiste en un órgano informativo del Presidente de la República en materia de seguridad nacional, teniendo entre sus funciones la de prevenir hechos que impliquen riesgo para la independencia o la integridad territorial o pongan en peligro la estabilidad del país y de sus instituciones.

XXXI. Que, mediante Decreto Ejecutivo N°37052-MICIT se establece en Costa Rica el Centro de Respuesta de Incidentes de Seguridad Informática denominado CSIRT-CR, con sede en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones MICITT, establecido en el año 2012.

XXXII. Que, el Decreto Ejecutivo N°37052-MICIT dispone que el CSIRT-CR tiene facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

XXXIII. Que, el 12 de abril de 2022 Costa Rica recibió un fuerte ataque cibernético a las bases de datos del Ministerio de Hacienda y en fechas posteriores se recibieron ataques a diferentes bases de datos de otras instituciones, tal como lo establece el Decreto Ejecutivo N°43542-MP-MICITT, *"Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información"*, en tal Decreto, se comprenden todas las acciones, obras y servicios necesarios para poder contener, solucionar y prevenir nuevos ataques en contra de los Sistemas de Información del Estado Costarricense.

XXXIV. Que, el artículo 2 del Decreto Ejecutivo Nº 44010-MICITT denominado "Plan Nacional de Atribución de Frecuencias (PNAF), dispone que, entre otros, son complemento de dicho PNAF, las leyes y reglamentos sobre telecomunicaciones y radiodifusión, las notas, referencias, resoluciones, recomendaciones y las indicaciones técnicas que surjan de la Unión Internacional de Telecomunicaciones (en adelante, UIT), los alcances y recomendaciones que se deriven y estén vigentes de la Convención Mundial de Telecomunicaciones, demás reglamentos dispuestos, así como el Convenio de la Unión Internacional de

Telecomunicaciones, ratificado por Costa Rica mediante la Ley Nº 8100 publicada en el Alcance Nº 44 al Diario Oficial La Gaceta Nº 114 de fecha 14 de junio de 2002, sin detrimento de que puedan ser adoptados de forma complementaria los documentos y/o recomendaciones de otros organismos regionales e internacionales generadores de estándares o desarrolladores de tecnología en materia de telecomunicaciones y radiodifusión, que sean consecuentes con la ciencia y la técnica, y debidamente justificados como aplicables a las necesidades del país.

XXXV. Que, la Organización Internacional de Normalización (del inglés, International Organization for Standardization, ISO) es una entidad reconocida mundialmente, dedicada a promover la estandarización y facilitar el intercambio de conocimientos técnicos y científicos para mejorar la cooperación en diversos campos.

XXXVI. Que específicamente en el ámbito de la seguridad de la información la Organización Internacional de Normalización ha emitido la familia de estándares ISO/IEC 27000 diseñados para ayudar a las organizaciones a establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, proporcionando un marco sólido y completo para abordar los riesgos relacionados con la seguridad, y ofreciendo a las organizaciones directrices claras sobre cómo establecer controles adecuados y eficaces para proteger la información.

XXXVII. Que, la Asociación de la Industria de las Telecomunicaciones (del inglés, Telecommunications Industry Association, TIA) es una organización reconocida a nivel internacional que promueve el desarrollo de estándares técnicos y normas en el campo de las telecomunicaciones y las tecnologías de la información.

XXXVIII. Que, de forma reciente la Asociación de la Industria de las Telecomunicaciones emitió el estándar SCS 9001, que proporciona directrices y requisitos específicos para garantizar la protección de los productos y servicios a lo largo de la cadena

de suministro, abordando aspectos clave como la gestión de riesgos, la evaluación y selección de proveedores, el control de acceso físico y lógico, la protección de datos y la gestión de incidentes, entre otros, promoviendo a través de su implementación, incrementar la confianza y la seguridad en las operaciones comerciales, así como fortalecer la reputación de las empresas y su competitividad en el mercado.

XXXIX. Que, en el año 2022, la Organización para la Cooperación y Desarrollo Económico (OCDE en lo sucesivo) publicó el Marco Político de la OCDE sobre Seguridad Digital – Ciberseguridad para la Prosperidad (del inglés, OECD Policy Framework on Digital Security – Cybersecurity for Prosperity), que evalúa las dimensiones económicas y sociales de la ciberseguridad e introduce las Recomendaciones de la OCDE sobre: gestión de riesgos de seguridad digital, estrategias nacionales de seguridad digital; seguridad digital de actividades críticas, seguridad digital de productos y servicios; y el tratamiento de vulnerabilidades de seguridad digital. Respecto a este último elemento, la Recomendación del Consejo sobre el Tratamiento de las Vulnerabilidades de Seguridad Digital (del inglés, Recommendation of the Council on the Treatment of Digital Security Vulnerabilities) recomienda establecer responsabilidades claras para todas las categorías de partes interesadas con respecto al tratamiento de vulnerabilidades, en particular, recomienda a los propietarios de vulnerabilidades minimizar la ventana de exposición a la explotación de vulnerabilidades por parte de criminales y otros actores maliciosos, procediendo lo más rápidamente posible, y asegurándose de que las mitigaciones sean suficientemente probadas para reducir al mínimo la probabilidad de crear nuevas vulnerabilidades y otros efectos secundarios negativos.

XL. Que, el citado Marco Político de la OCDE sobre Seguridad Digital– Ciberseguridad para la Prosperidad, recomienda a los responsables políticos que consideren la seguridad digital a nivel estratégico, abogando por la aplicación de una estrategia nacional con una visión clara para crear una cultura de seguridad digital y que

consideren la seguridad digital a nivel de mercado, abogando por que los responsables políticos *"fomenten o exijan que los operadores adopten medidas de gobernanza, protección, detección y respuesta, así como de resiliencia",* especialmente en el contexto de actividades críticas y recomienda a los responsables políticos que consideren la seguridad digital a nivel técnico para combatir las vulnerabilidades y los riesgos de la tecnología.

XLI. Que, en el año 2019 la Comisión Europea adoptó la *"Recomendación sobre la ciberseguridad de las redes 5G"* la cual insta a los Estados miembros a completar evaluaciones de riesgos nacionales y revisar las medidas nacionales en relación con la seguridad informática de las redes 5G, así como, trabajar a nivel de la Unión Europea (UE en lo sucesivo) en una evaluación de riesgos coordinada y preparar una caja de herramientas de posibles medidas de mitigación.

XLII. Que, a partir de lo anterior, en el mes de enero de 2020 la NIS Cooperation Group (Grupo de Cooperación de los Sistemas de Redes e Información por su traducción libre al español), publicó el documento denominado *"Ciberseguridad de Redes 5G - EU Caja de Herramientas para mitigación de riesgos",* consistente en un conjunto de medidas para mitigar los principales riesgos de ciberseguridad de las redes de quinta generación (5G) y proporciona además orientación para la elección de medidas, siendo esto un marco referencial sólido y consolidado que garantiza un nivel adecuado de ciberseguridad en las citadas redes. Entre los riesgos de ciberseguridad identificados en la caja de herramientas se contemplan los siguientes: *"dependencia de un único suministrador en determinadas redes o falta de diversidad a nivel nacional, intromisiones por parte de Estados a través de la cadena de suministro de la 5G, aprovechamiento de las redes 5G por parte de grupos de delincuentes organizados para atacar a usuarios finales, entre otros."*

XLIII. Que, como referencia internacional en el caso de España, se tiene el Real Decreto-ley 7/2022, de fecha 29 de marzo de 2022, denominado *"Sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de*

*quinta generación"*, que establece una serie de condiciones de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G). En particular, el numeral 12 del Real Decreto-ley 7/2022 contempla aspectos relacionados con la estrategia de diversificación en la cadena de suministro y el numeral 14 aborda las medidas estratégicas y aspectos relacionados con la exposición a injerencias externas de un tercer Estado.

XLIV. Que, de acuerdo con la Superintendencia de Telecomunicaciones mediante su dictamen N°09228-SUTEL-OTC-2022 de fecha 20 de octubre de 2022", en referencia a las redes de quinta generación (5G), ha manifestado, que:

> *"(…) prometen generar cambios en muchas industrias. La tecnología 5G es una gran innovación capaz de ayudar a muchas otras innovaciones complementarias a desarrollarse. Los aspectos más prometedores de la tecnología son el aumento de la capacidad (ancho de banda), el aumento de las velocidades de carga y descarga de datos, la disminución de la latencia (retraso) en las transmisiones de datos y una mayor eficiencia de entrada."*

XLV. Que, el Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027: "Costa Rica: Hacia la Disrupción Digital Inclusiva", establece la política pública en materia de telecomunicaciones el cual plantea dentro de sus metas la disminución de la brecha digital de conectividad y uso de los servicios móviles, acceso universal, servicio universal, solidaridad, y optimización del uso del espectro radioeléctrico en lo que respecta a su administración y planificación eficiente para destinarlo a las necesidades presentes y futuras de servicios de telecomunicaciones de todos los habitantes del país.

XLVI. Que, de conformidad con el ordinal 12 de la Ley General de Telecomunicaciones, Ley N°8642 en concordancia con los artículos 22 y 23 del Decreto Ejecutivo Nº34765-MINAET, “Reglamento a la Ley General de Telecomunicaciones”, el Poder Ejecutivo debe acreditar la necesidad y pertinencia de un eventual concurso público de bandas del espectro radioeléctrico para el desarrollo de sistemas IMT, incluyendo 5G.

XLVII. Que, derivado de lo anterior, la Superintendencia de Telecomunicaciones, mediante los dictámenes técnicos N° 05348-SUTEL-DGC-2019 de fecha 19 de junio de 2019, aprobado por su Consejo mediante el Acuerdo N° 033- 040-2019, adoptado en la sesión ordinaria N° 040-2019, celebrada en fecha 27 de junio de 2019; N° 10425-SUTEL-DGC-2019 de fecha 20 de noviembre de 2019, aprobado por su Consejo mediante el Acuerdo N° 020-076-2019, adoptado en la sesión ordinaria N° 076-2019, celebrada en fecha 25 de noviembre de 2019; N° 05071-SUTEL-DGC-2020 de fecha 09 de junio de 2020, aprobado por su Consejo mediante el Acuerdo N° 014-045-2020, adoptado en la sesión ordinaria N° 045-2020, celebrada en fecha 19 de junio de 2020; N° 00138-SUTEL-DGC-2021 de fecha 07 de enero de 2021, aprobado por el Consejo de la SUTEL mediante el Acuerdo N° 023-002-2021, adoptado en la sesión ordinaria N° 002-2021, celebrada en fecha 14 de enero de 2021, aclarado y ampliado mediante oficio Nº 02156- SUTEL-DGC-2021 de fecha 12 de marzo de 2021, aprobado por el Consejo de la SUTEL mediante el Acuerdo N° 011-021-2021, adoptado en la sesión ordinaria N° 021-2021, celebrada en fecha 18 de marzo de 2021; así como los oficios N° 04225- SUTEL-OTC-2021 de fecha 19 de mayo de 2021, aprobado por su Consejo, mediante el Acuerdo N° 031-041-2021, adoptado en la sesión ordinaria N° 041- 2021, celebrada en fecha 27 de mayo de 2021; N° 04482-SUTEL-DGC-2021 de fecha 28 de mayo de 2021, aprobado por su Consejo mediante el Acuerdo N° 022- 046-2021, adoptado en la sesión ordinaria N° 046-2021, celebrada el día 24 de junio de 2021; N° 01355-SUTEL-DGC-2023 de fecha 22 de febrero de 2023, aprobado por su Consejo mediante el Acuerdo N° 003-014-2023, adoptado en la sesión ordinaria N° 014-2023, celebrada en fecha 23 de

febrero de 2023, y N° 01556-SUTEL-OTC-2023, de fecha 22 de febrero de 2023, aprobado por su Consejo mediante el Acuerdo N° 004-014-2023, adoptado en la sesión ordinaria N° 014-2023, celebrada en fecha 23 de febrero de 2023, se acreditó la existencia de estudios necesarios por medio de la emisión de los informes técnicos conjuntos N° MICITT-DCNT-INF-012-2022 / N° MICITT-DEMT-INF-012-2022 / N° MICITT-DERRT-INF-009-2022 de fecha 31 de octubre de 2022, y N° MICITT-DCNT-INF-003-2023/N°MICITT-DEMT-INF-002-2023/N°MICITT-DERRT-INF-002-2023 ambos del Viceministerio de Telecomunicaciones (MICITT), y por tanto la viabilidad de dar la instrucción a la SUTEL para su inicio.

XLVIII. Que, el Poder Ejecutivo mediante el Acuerdo Ejecutivo N°031-2023-TEL-MICITT, publicado en el Alcance N° 77 al Diario Oficial La Gaceta N°75 de fecha 02 de mayo de 2023, emitió la instrucción a la Superintendencia de Telecomunicaciones para el inicio al concurso público de bandas del espectro radioeléctrico para el desarrollo de sistemas IMT, incluyendo 5G.

XLIX. Que, de forma complementaria el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, mediante oficio N°MICITT-DM-OF-416-2023, de fecha 19 de mayo de 2023, remitió a la SUTEL los *“Lineamientos técnicos adicionales de la Ministra Rectora en cumplimiento de lo dispuesto en el artículo 2 del Acuerdo Ejecutivo N° 031-2023- TEL-MICITT”*, mismo que, en el punto 3 *“Fines del Concurso*”, inciso k) *“Seguridad de las redes IMT-2020 y la privacidad de los usuarios de los servicios de telecomunicaciones”,* establece entre otras cosas que, dadas las implicaciones en materia de seguridad nacional, así como de la privacidad y seguridad de los usuarios de los servicios de telecomunicaciones, para la realización del proceso concursal de cita, se incorpore dentro de las condiciones técnicas de despliegue que se exijan a los eventuales adjudicatarios, los aspectos y estándares relativos a la seguridad de las redes móviles IMT-2020, incluyendo 5G, considerando para ello las distintas medidas técnicas, de gestión del riesgo, de arquitectura de red y de cadena de suministro que puedan generar vulnerabilidades de seguridad y privacidad de los usuarios finales de las redes de

telecomunicaciones, como fin primordial de esta medida, en protección de los principios de ley y de nivel constitucional, y se propicien entornos adecuados para fomentar la inversión, la innovación, y el desarrollo de infraestructura, y con ello alcanzar mayores niveles de bienestar en la sociedad.

L. Que, en el marco de tal concurso público y reconociendo que si bien la tecnología de quinta generación (5G) tiene la capacidad de generar numerosas oportunidades, también conlleva muchos riesgos y amenazas porque esta ofrece una mayor superficie de ataque que los sistemas de telecomunicaciones anteriores tales como tercera o cuarta generación, debido a su naturaleza y, en particular, a su dependencia de los programas informáticos, resulta necesario emitir una norma jurídica que garantice desde la óptica de las telecomunicaciones un despliegue, implementación y mantenimiento de las redes basadas en la tecnología de quinta generación (5G).

LI. Que, al tenor de lo indicado, es importante resaltar que a partir de la tecnología de quinta generación (5G) y su profunda integración en distintos procesos y aplicaciones, se trasiegan grandes cantidades de datos permitiendo almacenar información personal y sensible de los usuarios y en ese sentido los operadores y proveedores en Costa Rica tienen la obligación de garantizar el derecho a la intimidad, la privacidad y el secreto de las comunicaciones, así como de proteger la confidencialidad de la información que obtengan de sus clientes o de otros operadores. Esto conlleva la obligación de que los operadores o proveedores deben implementar medidas adecuadas de seguridad de la información para prevenir el acceso no autorizado a la información de los usuarios y evitar la filtración de datos sensibles e información protegida desde el ámbito de la intimidad y privacidad de estos.

LII. Que, la implementación de las redes basadas en la tecnología de quinta generación (5G), ha generado preocupaciones sobre la seguridad nacional y el riesgo de espionaje pues existe la posibilidad de que información confidencial y

sensible pueda ser interceptada y utilizada por agentes extranjeros para fines de espionaje. Por esta razón, la seguridad nacional debe ser una prioridad en la implementación de las redes 5G, y los gobiernos deben trabajar en estrecha colaboración con los operadores y proveedores para garantizar la seguridad y la integridad de la información que se transmite a través de estas redes. Esto implica la implementación de medidas de seguridad adecuadas y la vigilancia constante de posibles amenazas informáticas.

LIII. Que, el artículo 361 inciso 2) de la Ley N° 6227, Ley General de la Administración Pública establece que *"1) Se concederá audiencia a las entidades descentralizadas sobre los proyectos de disposiciones generales que puedan afectarlas.";* en este sentido el Poder Ejecutivo llevó a cabo las diligencias de consulta procedentes al Órgano Regulador y a la Autoridad Reguladora de Servicios Públicos considerando para tales efectos el carácter y la naturaleza de la materia tratada.

LIV. Que, mediante oficio MICITT-DM-OF-651-2023 de fecha 04 de agosto de 2023 se realizó consulta a la Junta Directiva de la Autoridad Reguladora de los Servicios Públicos y a la Superintendencia de Telecomunicaciones para que en el ámbito de sus competencias se refirieran al proyecto normativo, confiriéndole el plazo de diez días hábiles para recibir sus observaciones.

LV. Que, vencido el plazo conferido en el considerando anterior, el Consejo Directivo de la Superintendencia de Telecomunicaciones remitió el oficio Nº 06900-SUTEL-CS-2023 de fecha 17 de agosto de 2023, con fundamento en la Ley Nº 9736, Ley de Fortalecimiento de las Autoridades de Competencia de Costa Rica, con las consideraciones del anteproyecto de decreto ejecutivo. Consideraciones que fueron revisadas y analizadas para la emisión de la presente reglamentación.

LVI. Que mediante informe Nº MICITT-DGDCFD-INF-007-2023 de fecha 25 de agosto de 2023, emitido por la Dirección de Gobernanza Digital y Certificadores de Firma Digital, del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, denominado “Ciberseguridad en Redes 5G” se analizan las mejores prácticas implementadas por países, para promover la ciberseguridad en la operación y servicios de las redes 5G y superiores, y proponer un articulado técnico – jurídico, de conformidad con las competencias dispuestas para las autoridades sectoriales con fundamento en lo dispuesto en el numeral 42 de la Ley General de Telecomunicaciones, a fin de resguardar el régimen de derechos de los usuarios finales en cuanto a la intimidad, la privacidad y el secreto de las comunicaciones y la autodeterminación informativa. Dicho informe valoró las consideraciones realizadas por la Superintendencia de Telecomunicaciones mediante oficio Nº 06900-SUTEL-CS-2023 de fecha 17 de agosto de 2023.

LVII. Que, sobre esta materia la Procuraduría General de la República, en su dictamen vinculante N°C-022-89 de fecha 25 de enero de 1989 ha manifestado:

> *“(..) la gran mayoría de las situaciones de urgencia que se han presentado y se presentan en Costa Rica son atípicas. Ello debido a que las normas jurídicas que regulan tales situaciones no las precisan en grado suficiente como supuestos constitutivos de urgencia, así como tampoco contemplan el efecto o contenido que habrá de tener las medidas que se adopten; sino que dichas situaciones deben ser asumidas mediante el acto cuyo motivo está definido con harta imprecisión, el cual puede consistir en el hecho puro y simple de una necesidad apremiante, previsto sin ulterior especificación ni cualidad, y* ***en el cual el contenido del acto se deja en blanco para que la autoridad respectiva lo cubra y lo determine, caso por caso, dentro de una gama amplia de posibilidades****.*
>
> *(…)”*

LVIII. Que, mediante Resolución Nº 16359-2016 de fecha 04 de noviembre de 2016, la Sala Constitucional ha manifestado en relación con la materia de seguridad nacional del Estado lo siguiente: *"(…) El secreto de Estado es un límite al derecho de acceso a la información; Existe secreto de Estado, en términos generales, en materia de seguridad nacional, defensa nacional y relaciones exteriores, no sólo con otros Estados, sino con los demás sujetos de Derecho Internacional Público (...)"*

LIX. Que, por disposición del artículo 1 de la Ley N° 8488, Ley Nacional de Emergencias y prevención del riesgo, se establece que *"(…) regulará las acciones ordinarias, establecidas en su artículo 14, las cuales el Estado Costarricense deberá desarrollar para reducir las causas de las pérdidas de vidas y las consecuencias sociales, económicas y ambientales, inducidas por los factores de riesgo de origen natural y antrópico; así como la actividad extraordinaria que el Estado deberá efectuar en caso de estado de emergencia, para lo cual se aplicará un régimen de excepción";* régimen de excepción que actualmente se presenta en relación con lo dispuesto en el Decreto Ejecutivo N°43542-MP-MICITT, *"Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información"*.

LX. Que, adicionalmente la Ley N° 8488, Ley Nacional de Emergencias y prevención del riesgo establece en su numeral 4 una serie definiciones, que entre otras incluye:

> *"(…)*
> ***Riesgo**: Probabilidad de que se presenten pérdidas, daños o consecuencias económicas, sociales o ambientales en un sitio particular y durante un periodo definido. Se obtiene al relacionar la amenaza con la vulnerabilidad de los elementos expuestos.*

***Estado de emergencia**: Declaración del Poder Ejecutivo, vía decreto ejecutivo, con fundamento en un estado de necesidad y urgencia, ocasionado por circunstancias de guerra, conmoción interna y calamidad pública. Esta declaratoria permite gestionar, por la vía de excepción, las acciones y la asignación de los recursos necesarios para atender la emergencia, de conformidad con el artículo 180 de la Constitución Política.*

***Amenaza**: Peligro latente representado por la posible ocurrencia de un fenómeno peligroso, de origen natural, tecnológico o provocado por el hombre, capaz de producir efectos adversos en las personas, los bienes, los servicios públicos y el ambiente.*

***Desastre**: Situación o proceso que se desencadena como resultado de un fenómeno de origen natural, tecnológico o provocado por el hombre que, al encontrar, en una población, condiciones propicias de vulnerabilidad, causa alteraciones intensas en las condiciones normales de funcionamiento de la comunidad, tales como pérdida de vidas y de salud de la población, destrucción o pérdida de bienes de la colectividad y daños severos al ambiente.*

***Emergencia**: Estado de crisis provocado por el desastre y basado en la magnitud de los daños y las pérdidas. Es un estado de necesidad y urgencia que obliga a tomar acciones inmediatas con el fin de salvar vidas y bienes, evitar el sufrimiento y atender las necesidades de los afectados. Puede ser manejada en tres fases progresivas: respuesta, rehabilitación y reconstrucción; se extiende en el tiempo hasta que se logre controlar definitivamente la situación.*

***Gestión del riesgo**: Proceso mediante el cual se revierten las condiciones de vulnerabilidad de la población, los asentamientos*

*humanos, la infraestructura, así como de las líneas vitales, las actividades productivas de bienes y servicios y el ambiente. Es un modelo sostenible y preventivo, al que incorporan criterios efectivos de prevención y mitigación de desastres dentro de la planificación territorial, sectorial y socioeconómica, así como a la preparación, atención y recuperación ante las emergencias.*

*(…)*

LXI. Que, en el contexto que atraviesa el país debido al estado de emergencia ocasionado por los ciberataques sufridos a nivel nacional, el Poder Ejecutivo reconoce la necesidad de fortalecer y adaptar el marco regulatorio sectorial mediante el aseguramiento de medidas técnico-jurídicas de carácter normativo, con un enfoque basado en el riesgo para la atención de riesgos de ciberseguridad, con la finalidad de garantizar la operación y explotación segura por quienes operen redes y presten servicios de telecomunicaciones sustentados en la tecnología de quinta generación (5G).

LXII. Que por la materia tratada se debe considerar que el artículo 1) de la Ley de Protección al ciudadano del exceso de requisitos y trámites administrativos, Ley N°8220, excluye de su ámbito de aplicación los trámites y procedimientos en materia de defensa del Estado y seguridad nacional.

LXIII. Que el acceso y disfrute de los servicios de las telecomunicaciones dentro de la Sociedad de la Información y el Conocimiento, requiere la adopción de un ordenamiento sectorial que resguarde de manera efectiva el régimen jurídico especial de protección a los derechos de los usuarios finales, sobre todo en su ámbito de intimidad, privacidad y secreto de las comunicaciones y la autodeterminación informativa.

**POR TANTO,**

**DECRETAN:**

# REGLAMENTO SOBRE MEDIDAS DE CIBERSEGURIDAD APLICABLES A LOS SERVICIOS DE TELECOMUNICACIONES BASADOS EN LA TECNOLOGÍA DE QUINTA GENERACIÓN MÓVIL (5G) Y SUPERIORES

## CAPÍTULO I
## Disposiciones Generales

**Artículo 1º-Objeto**. El presente reglamento tiene por objeto establecer medidas de ciberseguridad para garantizar el uso y la explotación segura y con resguardo de la privacidad de las personas, de las redes y los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores.

**Artículo 2º-Ámbito de aplicación.** Está sometida al presente reglamento la operación activa de redes y servicios basados en la tecnología de quinta generación móvil (5G) y superiores, por parte de las personas físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que operen redes o presten servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores que se originen, terminen o transiten por el territorio nacional, exceptuando la operación de redes privadas de telecomunicaciones.

En el caso de procesos de compra pública que tengan por objeto la habilitación de redes y servicios basados en la tecnología de quinta generación móvil (5G) y superiores, así como de equipamiento tecnológico activo necesario para el despliegue de éstas, para el uso y explotación del espectro radioeléctrico, la Administración o entidad contratante deberá adoptar los mecanismos idóneos para verificar que los potenciales oferentes han considerado todos los aspectos alusivos a la gestión y mitigación de riesgos contenidos en la presente normativa, a la hora de planificar, diseñar e implementar su oferta técnica. En caso de resultar adjudicatario, las disposiciones de la presente norma serán de acatamiento obligatorio durante la operación de las redes y prestación de los servicios basados en la tecnología de quinta generación móvil (5G) o superiores.

**Artículo 3º-Definiciones.** Para efectos del presente Decreto Ejecutivo se entenderá por:

a) **5G**: Quinta generación de sistemas de redes de telecomunicaciones móviles internacionales.

b) **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

c) **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. Este análisis proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de estos.

d) **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

e) **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

f) **Cadena de suministro:** Un sistema de organizaciones, personas, tecnología, actividades, información y recursos involucrados en el traslado de un producto o servicio del proveedor al cliente.

g) **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física.

h) **Ciberseguridad:** Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

i) **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

j) **Nivel de riesgo:** Magnitud de un riesgo expresado en relación con la combinación de consecuencias y su probabilidad.

k) **Red 5G**: Red de telecomunicaciones de conformidad con lo establecido en el artículo 6), inciso 19) de la Ley General de Telecomunicaciones, Ley Nº8642 utilizada para la prestación de servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G).

l) **Riesgo**: Combinación de las consecuencias de un evento y la probabilidad asociada de ocurrencia. En el contexto de la seguridad de la información, el riesgo se refiere a la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o un grupo de activos de información y, por lo tanto, causen daño a una organización.

m) **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información. Tiene como característica la autenticidad, el no repudio y la confiabilidad.

n) **Servicio público esencial**: Se entiende por servicio público esencial, aquél cuya paralización ponga en peligro los derechos a la vida, la salud y la seguridad pública, el transporte, mientras el viaje no termine, y la carga y

descarga en muelles y atracaderos, cuando se trate de bienes de los cuales dependa, directamente, la vida o la salud de las personas. Esa categoría incluye, entre otros, los de telecomunicaciones necesarios para la prestación eficaz de los demás servicios públicos, de conformidad con lo establecido en el Reglamento al artículo 375 del Código de Trabajo, Decreto Ejecutivo N° 38767-MP-MTSS-MJP.

o) **Suministradores de hardware y software:** Entidades que brindan servicios o equipo activo a los sujetos comprendidos en el artículo 2 del presente reglamento. Esta categoría incluye: i) fabricantes de equipos de telecomunicaciones; y ii) otros proveedores externos, como proveedores de infraestructura en la nube, integradores de sistemas, contratistas de seguridad y mantenimiento, y fabricantes de equipos de transmisión, cuando estos se encargan de configurar e integrar los equipos activos y software de la solución.

p) **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## CAPÍTULO II
## De los Riesgos

**Artículo 4º- Riesgos Nacionales de Ciberseguridad en Redes 5G y Superiores.** Para garantizar un uso y explotación segura de las redes y la prestación de los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores, se han identificado los siguientes riesgos nacionales de ciberseguridad de las redes 5G y superiores, agrupados en cinco escenarios. Tales riesgos conformarán el marco de referencia para establecer lineamientos de política pública y medidas regulatorias siguiendo un enfoque basado en la prevención, mitigación y control del riesgo:

| | |
|---|---|
| I Escenarios de riesgo relacionados con medidas de seguridad insuficientes | R1: Fallos de configuración de las redes.<br>R2: Controles de acceso insuficientes. |
| II Escenarios de riesgo relacionados con la cadena de suministro de la 5G. | R3: Productos de baja calidad.<br>R4: Dependencia de un único suministrador en determinadas redes o falta de diversidad a nivel nacional, cuando este se encarga de configurar e integrar todos los equipos activos y software de la solución, o si la red está compuesta por equipos activos y software de un único fabricante. |
| III Escenarios de riesgo relacionados con el *modus operandi* de los principales agentes de riesgo | R5: Intromisiones por parte de Estados a través de la cadena de suministro de la 5G, cuando esto pueda comprometer la seguridad, disponibilidad, integridad y privacidad de la información.<br>R6: Aprovechamiento de las redes 5G por parte de grupos de delincuentes organizados para atacar a usuarios finales. |
| IV Escenarios de riesgo relacionados con las interdependencias entre las redes 5G y otros sistemas críticos | R7: Daños significativos a infraestructuras o servicios críticos.<br>R8: Caída general de las redes debido a la interrupción de suministro eléctrico u otros sistemas de soporte. |
| V Escenarios de riesgo relacionados con dispositivos de los usuarios finales | R9: Utilización abusiva del Internet de las cosas, microteléfonos o dispositivos inteligentes. |

## CAPÍTULO III
## Gestión y Mitigación de los Riesgos

**Artículo 5º- Mitigación de los Riesgos Nacionales de Ciberseguridad Redes 5G y Superiores.** Los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este decreto reglamentario–deberán acatar las medidas de mitigación de los riesgos nacionales contenidas en el presente Capítulo, las cuales son de índole estratégico y técnico.

El Poder Ejecutivo podrá actualizar tales medidas conforme con los avances tecnológicos, la emisión de nuevos estándares, y demás criterios que resulten pertinentes. No obstante, deberá garantizar la seguridad jurídica de las inversiones y actuar sin detrimento de los derechos adquiridos y situaciones jurídicas consolidadas.

**Artículo 6º- Adopción de estándares.** Los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Decreto Ejecutivo, deberán adoptar, implementar, y mantener estándares y/o marcos de referencia sobre ciberseguridad, incluyendo los siguientes:

| Número | Nombre |
|---|---|
| ISO/IEC 27001:2022 | Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Sistemas de Gestión de la Seguridad de la Información — Requerimientos |
| ISO/IEC 27002:2022 | Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Controles de seguridad de la información |
| ISO/IEC 27003:2017 | Tecnologías de la información —Técnicas de seguridad — Sistemas de Gestión de la Seguridad de la Información —Guía |

| | |
|---|---|
| ISO/IEC 27011:2016 | Tecnologías de la información —Técnicas de seguridad — Código de prácticas para los controles de seguridad de la información basado en ISO/IEC 27002 para organizaciones de telecomunicaciones. |
| SCS 9001 | Estándar de Seguridad de la Cadena de Suministro y Ciberseguridad |

**Artículo 7º**- **Análisis de Riesgos de las Redes 5G y Superiores.** Los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este reglamento, deberán analizar los riesgos de ciberseguridad de sus redes detectando vulnerabilidades y amenazas.

El análisis de riesgos de las Redes 5G y superiores, deberá realizarse de oficio una vez identificado el riesgo alto de conformidad con los parámetros definidos en el artículo 10 del presente Reglamento.

El análisis de riesgos deberá incluir los siguientes elementos:

1) Funciones del núcleo de la red,
2) Funciones de transporte y transmisión,
3) La red de acceso,
4) Los sistemas de control y gestión y los servicios de apoyo,
5) Las funciones de computación en el borde, virtualización de red y gestión de sus componentes, y
6) Los relativos a intercambios de tráfico con redes externas e Internet.

El análisis de riesgos deberá incluir los siguientes factores:

a) Parametrización y configuración de elementos y funciones de red.
b) Políticas de integridad y actualización de los programas informáticos.

c) Estrategias de permisos de acceso a activos físicos y lógicos.
d) Dependencias de determinados suministradores en elementos críticos de la red 5G y superiores.
e) Agentes externos, incluyendo grupos organizados con capacidad para atacar la red.
f) Equipos terminales y dispositivos conectados a la red.
g) Redes externas conectadas a la red 5G y superiores.
h) La interrelación con los servicios públicos esenciales.

El análisis de riesgos deberá, además, incluir una priorización y jerarquía de los riesgos en función de los siguientes parámetros:

i. Afectación a un elemento crítico de la red pública 5G o superior.
ii. Tipo de recurso, infraestructura y servicio que pueda verse afectado.
iii. Afectación a la integridad y mantenimiento técnico de la red o a la continuidad del servicio.
iv. Capacidad de detección y recuperación.
v. Número y tipo de usuarios afectados.
vi. Tipo de información cuya integridad haya podido verse comprometida.

Lo anterior, sin perjuicio del ejercicio de las potestades de control y fiscalización superior por parte de las autoridades sectoriales cada una en su ámbito de competencia.

**Artículo 8º**- **Gestión del Riesgo de las Redes 5G y Superiores.** Los sujetos comprendidos en el ámbito de aplicación definido en el artículo 2 de este Reglamento, deberán adoptar las medidas adecuadas para gestionar los riesgos identificados de conformidad con el artículo 7 de esta normativa.

Para estos efectos se deberán de incluir las siguientes medidas:

a) Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o superiores, o cualesquiera de sus elementos, así como la continuidad en la prestación de servicios de telecomunicaciones móviles.
b) Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de los servicios públicos esenciales.
c) Seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento adecuado de registros de acceso.
d) Mantener las credenciales de usuario para el acceso a la red en posesión de los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento.
e) Cumplir con la implementación de los estándares señalados en el artículo 6 del presente Reglamento.
f) Someterse, asumiendo su costo, a una auditoría de ciberseguridad realizada por una entidad pública o una entidad privada, acreditada según el estándar correspondiente del artículo 6 del presente reglamento, cuando sea requerido, así como, proveer la información necesaria para la elaboración de la citada auditoría. Una vez comunicados los resultados de esta auditoría deberán de informarse en el plazo de diez días hábiles a partir de su recibo a las autoridades sectoriales, para que cada una proceda con su análisis en el ámbito de sus competencias de conformidad con lo dispuesto en el artículo 42 de la Ley N°8642, Ley General de Telecomunicaciones.
g) Exigir a sus suministradores de hardware y software involucrados en las redes 5G y superiores el cumplimiento de estándares de ciberseguridad, desde el diseño de los productos y servicios hasta su puesta en funcionamiento.
h) Controlar su propia cadena de suministro para garantizar una operación y explotación segura de las redes de telecomunicaciones móviles y sus servicios.

i) Diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red 5G o superior, de forma tal que dichos equipos, sistemas o recursos sean proporcionados, como mínimo, por dos suministradores de hardware y software diferentes.

**Artículo 9º**- **Análisis y Gestión del Riesgo en la Cadena de Suministro**. Los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento, deberán solicitar a sus suministradores de hardware y software, que intervienen en el funcionamiento y operación de las redes 5G y superiores y sus servicios, la definición de los requisitos, controles y mediciones del sistema de gestión de ciberseguridad de la cadena de suministro para el diseño, desarrollo, producción, entrega, instalación y mantenimiento de hardware, software y servicios de conformidad con el estándar SCS 9001 “Estándar de Seguridad de la Cadena de Suministro y Ciberseguridad”.

Dicha información deberá de ser presentada atendiendo a las particularidades de los procesos dispuestos por el Poder Ejecutivo y la Superintendencia de Telecomunicaciones (Sutel), cada una de acuerdo con su ámbito de competencia, sin detrimento del ejercicio de las potestades de control y fiscalización superior para verificar el cumplimiento de estas disposiciones.

En el caso de los procesos de contratación pública promovidos por entidades contratantes, que tengan por objetivo la operación de redes y servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) o superiores, incorporarán lo dispuesto en el presente artículo en las reglas de la contratación con el fin de garantizar el uso y la explotación segura de las redes y los servicios de telecomunicaciones y con resguardo de la intimidad y la privacidad de los usuarios finales.

**Artículo 10º**- **Parámetros de riesgo alto.** Los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento, deberán considerar los siguientes parámetros de riesgo alto para la operación de redes de telecomunicaciones 5G o superiores y la prestación de sus servicios:

a) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento cuenten con un único suministrador de hardware y software en su cadena de suministro, cuando este se encarga de configurar e integrar todos los equipos activos y software de la solución, o si la red está compuesta por equipos activos y software de un único fabricante.
b) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento o sus suministradores de hardware y software tengan algún informe de incidente publicado por el CSIRT-CR sobre brechas en la ciberseguridad de sus sistemas que no han sido atendidas y por ende implican un riesgo para la seguridad, disponibilidad, integridad o privacidad de la información de los usuarios finales.
c) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento o sus suministradores de hardware y software sean susceptibles de presión por parte de un gobierno extranjero por disposición normativa o política pública oficial de dicho gobierno extranjero, en relación con la ubicación o ejecución de sus operaciones.
d) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento o sus suministradores de hardware y software tienen su base en un país, o, de alguna manera, están sujetos a la dirección de un gobierno extranjero con leyes o prácticas establecidas que les puedan requerir que compartan la información de los usuarios finales de servicios de telecomunicaciones en ausencia de un proceso legal transparente que proteja adecuadamente sus derechos e intereses.

e) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento utilizan suministradores de hardware y software que tengan su sede en un país que no ha manifestado su consentimiento de obligarse al cumplimiento del Convenio sobre Ciberdelincuencia (Convenio de Budapest).
f) Cuando los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este reglamento utilizan suministradores de hardware y software que no cumplen con los estándares de ciberseguridad dispuestos en el artículo 6 de este Reglamento.

**Artículo 11º. Medidas aplicables ante la identificación de riesgo alto.** Cuando alguno de los sujetos comprendidos en el ámbito de aplicación del artículo 2 del presente Reglamento identifique la presencia de alguno o varios de los parámetros de riesgo alto consignados en el artículo anterior, deberá informarlo a la Superintendencia de Telecomunicaciones (Sutel) de conformidad con las disposiciones del artículo 42 de la Ley General de Telecomunicaciones, Nº8642, dentro de los 3 (tres) días naturales siguientes a su identificación y adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de sus redes y sus servicios.

Cuando se identifique la presencia de alguno o varios de los parámetros de riesgo alto por parte de los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento, quedará sujeto a la adopción inmediata de las siguientes medidas técnicas de ciberseguridad:

1) No podrán ser utilizados en elementos críticos de la red, equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales por representar un alto riesgo de ciberseguridad para las redes 5G y superiores, y la seguridad nacional. Para tal efecto, se declaran elementos críticos de la red 5G y superiores los siguientes:

i. Los relativos a las funciones del núcleo de la red.
ii. Los sistemas de control y gestión y los servicios de apoyo.
iii. La red de acceso en aquellas zonas geográficas y ubicaciones que proporcionen cobertura a centros vinculados con la seguridad nacional y la provisión de servicios públicos esenciales.

2) Llevar a cabo la sustitución de los equipos, productos y servicios de la red 5G y superiores cuando ello fuera necesario, para lo cual, deberá tener en cuenta la situación del mercado de los suministradores de hardware y software, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G y superiores, especialmente en los elementos críticos de la red, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, así como su impacto económico. En ningún caso, el plazo de sustitución de los equipos podrá ser superior a cinco años, contados a partir de la clasificación como de alto riesgo.

El cumplimiento de las presentes disposiciones reglamentarias deberá ser consideradas para la operación de redes 5G y superiores y sus servicios, de conformidad con las disposiciones del artículo 49 numerales 1 y 3 de la Ley N°8642, Ley General de Telecomunicaciones.

## CAPÍTULO IV
## Disposiciones finales

**Artículo 12º— Confidencialidad de la información.** Por tratarse de materia de seguridad nacional, y la protección a los derechos fundamentales de intimidad, la privacidad y el secreto de las comunicaciones, y la autodeterminación informativa de los usuarios finales, la información suministrada por los sujetos comprendidos en el ámbito de aplicación del artículo 2 de este Reglamento, sobre el análisis y gestión

de riesgos de las redes, el análisis y gestión de riesgos de la cadena de suministro, el informe de auditoría de ciberseguridad y los parámetros de riesgo alto, deberán ser tratados con carácter confidencial, de forma que no podrán ser utilizadas para una finalidad distinta al cumplimiento del presente Reglamento.

**Artículo 13º— Sanciones e infracciones.** El régimen sancionatorio administrativo aplicable por el incumplimiento de las disposiciones contenidas en este Decreto Ejecutivo se regirá por lo dispuesto en la Ley Nº 8642, Ley General de Telecomunicaciones.

**Artículo 14º- Declaratoria de interés público.** Se declara de interés público el establecimiento de medidas de ciberseguridad para garantizar la operación segura de redes de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores y sus servicios.

**Artículo 15º— Vigencia.** Rige a partir de su publicación en el Diario Oficial La Gaceta.

**Transitorio Único.** En un plazo de 15 meses, a partir de la publicación del presente Decreto Ejecutivo, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones publicará los lineamientos de buenas prácticas en materia de Ciberseguridad para redes 4G y generaciones anteriores.

Dado en la Presidencia de la República. — San José, a los 25 días del mes de agosto del año dos mil veintitrés.

RODRIGO CHAVES ROBLES.—El Ministro de Seguridad Pública, Mario Zamora Cordero y la Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones, Paula Bogantes Zamora.—1 vez.—O. C. N° 006-2023-TEL.—Solicitud N° 4600076150.—( D44196 - IN2023806908 ).

**N° 44182-MTSS**

**EL PRESIDENTE DE LA REPÚBLICA**
**Y EL MINISTRO DE TRABAJO Y SEGURIDAD SOCIAL**

En el ejercicio de las facultades que les confieren los numerales 140 incisos 3) y 18) y 146 de la Constitución Política de la República de Costa Rica, del 7 de noviembre de 1949; los artículos 25 inciso 1), 27 inciso 1), 28 inciso 2) acápite b) y 103 de la Ley General de la Administración Pública, No. 6227 del 2 de mayo de 1978.

**CONSIDERANDO:**

I. Que mediante Decreto Ejecutivo No. 34306-MTSS del 05 de diciembre de 2007, se dictó el Reglamento del Sistema Institucional de Archivos del Ministerio de Trabajo y Seguridad Social, con el fin de organizar y regular el funcionamiento del sistema de archivos del Ministerio de Trabajo y Seguridad Social (SIAR-MTSS).

II. Que mediante Directriz DMT-032-2015 del 03 de diciembre de 2015, en el Ministerio de Trabajo y Seguridad Social se puso en marcha un sistema de gestión documental y control de gestión, para la digitalización de la documentación existente y de la automatización de procesos que permitan la prestación de servicios más efectivos, ágiles y accesibles a la ciudadanía.

III. Que mediante Decreto Ejecutivo No. 40554-C, del 29 de junio de 2017, denominado Reglamento a la Ley del Sistema Nacional de Archivos, se actualizó la reglamentación a la Ley del Sistema Nacional de Archivos, No. 7202, del 24 de octubre de 1990, estableciendo pautas más claras para el cumplimiento de los objetivos de dicha Ley.

IV. Que mediante Decreto Ejecutivo No. 41059-MTSS, del 06 de abril de 2018, se modificó la estructura, organización y funcionamiento del Ministerio de Trabajo y Seguridad Social, para adecuarla a la estructura orgánico funcional, en el que el Departamento de Archivo Central dependerá de la Dirección General Administrativa y Financiera.

V. Que el uso de documentos electrónicos, certificados y firmas digitales; la modificación de la estructura, organización y funcionamiento del Ministerio de Trabajo y Seguridad Social; una adecuada aplicación de normas jurídicas mediante la promulgación del reglamento a la Ley del Sistema Nacional de Archivos, así como el mantenimiento del control interno del archivo institucional, hacen necesaria la reforma al Reglamento del Sistema Institucional de Archivos del Ministerio de Trabajo y Seguridad Social, para adecuarlo a los cambios tecnológicos y normativas establecidas.

VI. Que, de conformidad con el Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Decreto Ejecutivo número 37045-MEIC, del 22 de febrero de 2012 y sus reformas, se determinó que la presente propuesta no establece ni modifica trámites, requisitos o procedimientos que el administrado deba cumplir, por lo que no se procedió con el trámite de control previo.

**POR TANTO:**

**DECRETAN:**

**REFORMA AL "REGLAMENTO DEL SISTEMA INSTITUCIONAL DE ARCHIVOS DEL MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL, DECRETO EJECUTIVO No. 34306-MTSS"**

**Artículo 1**.- Refórmense los artículos 2, 3, 4; 6, 7, 9, 10, 16, 28, 30, 31, 32; 33, 34, 35, 38, 41, 42, 44 y 45, el nombre del Capítulo VII y adiciónese un nuevo artículo 49 corriéndose la numeración de los actuales artículos 49 y 50 de manera que se numeren como artículos 50 y 51 del "Reglamento del Sistema Institucional de Archivos del Ministerio de Trabajo y Seguridad Social", Decreto Ejecutivo No. 34306-MTSS del 5 de diciembre de 2007, para que en lo sucesivo se lean así:

*"**Artículo 2°-**El SIAR-MTSS estará conformado por el Archivo Central como órgano rector, los archivos de gestión de las diferentes Unidades Administrativas, excepto los órganos adscritos que debido a su grado de desconcentración tienen independencia funcional, los archivos especializados, archivos periféricos o de Oficinas Regionales y el Comité Institucional de Selección y Eliminación de Documentos.*

***Artículo 3°-** El Archivo Central es una Unidad dependiente de la Dirección General Administrativa y Financiera.*

***Artículo 4°-** Definición de términos archivísticos para la aplicación del presente reglamento:*

***ACERVO DOCUMENTAL.** Conjunto de documentos de un archivo.*

***ACTA DE ELIMINACIÓN DE DOCUMENTOS.*** *Documento en el que constan todos los tipos documentales que se eliminan.*

***ARCHIVO.*** *Secciones de entidades donde se reúnen, conservan, clasifican, ordenan, describen, seleccionan, administran y facilitan los documentos textuales, gráficos, audiovisuales y legibles por máquina, producidos por los individuos y las instituciones como resultado de sus actividades y que son utilizados por parte de la administración y para la investigación.*

***ARCHIVO CENTRAL.*** *Es una unidad que administra, custodia y conserva los documentos en cualquier soporte con valor administrativo, legal, permanente e histórico que son transferidos por las diferentes oficinas del Ministerio de Trabajo y Seguridad Social de acuerdo con el informe de valoración emitido por la Dirección General del Archivo Nacional, con el fin de brindar el servicio a las personas usuarias.*

***ARCHIVO ESPECIALIZADO.*** *Son todos aquellos archivos que se especializan en una materia en específico; estos generalmente están compuestos por expedientes.*

***ARCHIVOS DE GESTION.*** *Los Archivos de Gestión son los que se establecen y organizan en cada una de las instancias contempladas en el Estatuto Orgánico del Ministerio de Trabajo y Seguridad Social, y son parte del SIAR-MTSS.*

***ARCHIVO HISTÓRICO.*** *Es el archivo que conserva permanentemente la documentación con valor histórico cultural para fines de investigación, la ciencia y la cultura.*

***ARCHIVOS PERIFÉRICOS.*** *Son los archivos desconcentrados o adyacentes de las Oficinas Centrales del Ministerio de Trabajo y Seguridad Social.*

***CICLO VITAL DEL DOCUMENTO.*** *Etapas sucesivas por las que atraviesan los documentos desde su producción o recepción en la oficina y su conservación temporal, hasta su eliminación o integración a un archivo permanente. Existen tres fases en el ciclo vital: creación, reproducción, selección o eliminación.*

***CLASIFICACIÓN.*** *Técnica mediante la cual se identifican y agrupan documentos semejantes con características comunes, de acuerdo con un plan establecido.*

***CLASIFICACIÓN ORGÁNICA.*** *Consiste en la utilización de la estructura orgánica de la institución para clasificar los documentos.*

***CLASIFICACIÓN POR FUNCIONES.*** *Consiste en la clasificación de los documentos, de acuerdo con las funciones y actividades de la institución.*

***CLASIFICACIÓN POR ASUNTOS O MATERIAS.*** *Consiste en la clasificación de los documentos, basada en los asuntos o materias a que se refieren.*

***CNSED:*** *Comisión Nacional de Selección y Eliminación de Documentos.*

***DEPÓSITO DE ARCHIVO.*** *Espacio que reúne las condiciones óptimas para la conservación de los documentos.*

***DOCUMENTO.*** *Son los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y en general todo objeto mueble que tenga carácter representativo o declarativo.*

***DOCUMENTOS DE ARCHIVO.*** *Son aquellos que se producen y reciben las diferentes instituciones en función de sus actividades, con la característica de ser documentos únicos. Con excepción de libros, revistas, periódicos, y otras publicaciones múltiples, los cuales se consideran material de biblioteca o centros documentales.*

***DOCUMENTO DIGITALIZADO.*** *Es la información consignada en forma analógica en una secuencia de valores numéricos, es decir, en una representación electrónica que se puede almacenar y acceder por medio de una computadora. Fotografiar electrónicamente una información, dividiéndola en miles de elementos llamados píxeles, representados por ceros y unos.*

***DOCUMENTO ELECTRÓNICO.*** *Soporte magnético, óptico, etc. Símbolos binarios que deben descifrarse. El contenido puede separarse del soporte. La estructura física no es evidente. Se requiere de una estructura lógica (un software y hardware). Los megadatos administrativos, funcionales y técnicos de los documentos producidos por medios automáticos deben ser conservados para su posterior identificación.*

***DOCUMENTOS OFICIALES***. *Son los que se producen y reciben en las oficinas de la Administración Pública, identificados cada uno con la fecha, el nombre impreso del remitente, la firma y el sello, aquel documento electrónico que tiene lógicamente asociada una firma digital certificada o documentos escaneados que cumplen con las normas técnicas de archivo emitidas por el ente Rector.*

***DOCUMENTOS DE USO RESTRINGIDO.*** *Son los que tienen información de carácter confidencial.*

***ELIMINACIÓN.*** *Es la destrucción física de los documentos que han perdido su valor administrativo, jurídico, legal, fiscal o contable y que no tienen valor histórico, permanente o que carecen de relevancia para la ciencia y la tecnología.*

***EXPEDIENTE.*** *Conjunto de documentos relacionados entre sí por un mismo asunto, que constituyen una unidad documental.*

***FECHAS EXTREMAS.*** *Se refiere a la fecha más antigua y a la más reciente de los documentos que pueden encontrarse en un expediente o en cualquier unidad documental.*

***FOLIACIÓN.*** *Es la operación incluida en los trabajos de ordenación que consiste en numerar consecutivamente cada pieza documental.*

***FONDO DOCUMENTAL.*** *Es la totalidad de los documentos que se producen, reciben y custodian en una oficina, institución o familia.*

***INFORME DE VALORACIÓN DE DOCUMENTOS.*** *Es un informe emitido por la Comisión Nacional de Selección y Eliminación de Documentos del Archivo Nacional donde se especifica los tipos documentales, las fechas extremas, la caducidad administrativa, el cual sirve para saber el valor asignado a cada tipo documental.*

***LISTAS DE REMISIÓN.*** *Instrumento descriptivo que se utiliza para anotar los. documentos que se trasladan de un archivo a otro.*

***MTSS:*** *Ministerio de Trabajo y Seguridad Social*

***MIGRACIÓN:*** *Proceso de transferir documentos electrónicos de un entorno de software/hardware o soporte de almacenamiento a otro entorno o soporte de almacenamiento con poca o ninguna alteración de su estructura, y sin alteración del contenido y contexto.*

***ORDENACIÓN.*** *Es la asignación de números o letras que se da a los documentos, así como su colocación en el espacio físico correspondiente.*

***PATRIMONIO DOCUMENTAL.*** *Conjunto de documentos conservados por su valor científico cultural.*

***PRINCIPIO DE ORDEN ORIGINAL.*** *Establece que no se debe alterar la ordenación de los documentos según estos van llegando a la serie documental.*

***PRINCIPIO DE PROCEDENCIA.*** *Es la custodia y conservación de las series. documentales según la procedencia de estos.*

***SELECCIÓN DE DOCUMENTOS.*** *Procedimiento intelectual en el cual se analiza el valor de los documentos en sus diferentes etapas y se determina su eliminación o su conservación.*

***SERIE DOCUMENTAL.*** *Conjunto de unidades documentales (carpetas) que forman parte de los grupos o subgrupos de un fondo y se caracterizan por tener elementos semejantes entre sí.*

***SIGNATURA.*** *Numeración correlativa por la que se identifican todas las unidades de conservación de un depósito.*

***SIAR:*** *Sistema Institucional de Archivos.*

***TABLA DE PLAZOS DE CONSERVACIÓN DE DOCUMENTOS.*** *Es un instrumento en el que constan todos los tipos documentales producidos o recibidos en una oficina o institución, en el cual se anotan todas sus características y se fija el valor administrativo y legal.*

***TIPO DOCUMENTAL.*** *Unidad documental producida por un organismo en el desarrollo de una competencia concreta regulada por una norma de procedimiento cuyo formato contenido informativo y soporte son homogéneos. Es el nombre que se le da a los documentos.*

***TRANSFERENCIA DE DOCUMENTOS.*** *Es transferir los documentos de los archivos.*

***UNIDAD DOCUMENTAL.*** *Elemento básico de una serie documental que puede estar constituido por un solo documento o por varios que forman un expediente.*

***UNIDAD EJECUTORA.*** *Entiéndase como la unidad académica, administrativa, productora de documentos.*

***VALOR ADMINISTRATIVO.*** *Es aquel valor que posee un documento para la administración que lo originó o para aquella que le sucede, como testimonio de sus procedimientos y actividades.*

***VALOR CONTABLE.*** *Es la utilidad o aptitud de los documentos que soportan el conjunto de cuentas, registros de los ingresos, egresos y de los movimientos económicos de una entidad pública o privada.*

***VALOR FISCAL.*** *Es la utilidad o aptitud que tienen los documentos para el tesoro o hacienda pública.*

***VALOR LEGAL.*** *Aquel que tienen los documentos que sirven de testimonio ante la ley.*

***VALORACIÓN DE DOCUMENTOS.*** *Proceso por el cual se determina el valor de los documentos con el fin de establecer su permanencia en las diferentes fases de archivo.*

***Artículo 6°-*** *Las funciones de las personas encargadas de los archivos de gestión, serán además de las contempladas en este artículo, las que se instruyan mediante los procedimientos e instructivos que se emitan para tal fin, y que lleve el Archivo Central.*

*a) Administrar los documentos con base en la Ley N° 7202 y su reglamento, leyes conexas y de acuerdo con las directrices emanadas por la Dirección General del Archivo Nacional y por el Archivo Central del MTSS, de manera que sirvan para la toma de decisiones, transparencia administrativa, rendición de cuentas, control interno, apoyo legal, administrativo y para la memoria documental institucional.*

*b) Verificar la validez de las firmas e integridad de los documentos recibidos y firmados digitalmente.*

*c) Llevar un control estricto del número consecutivo que le corresponde a cada tipo documental utilizando los sistemas automatizados y formales del MTSS para la toma de consecutivos, archivo de documentos, gestión y conservación de documentos electrónicos con firma digital avanzada avalados por el Archivo Central.*

*d) Ordenar y archivar la documentación según la clasificación orgánico funcional o por tipología documental, asuntos o materias en forma cronológica y consecutiva según sea el archivo de gestión.*

*e) Conformar expedientes en forma cronológica y consecutiva, debidamente identificados con el nombre o asunto y foliados.*

*f) Coordinar con el Archivo Central la confección y actualización de tablas de plazos de conservación de documentos según lo establecido por la Ley No. 7202 y su reglamento.*

*g) Comunicar al Archivo Central cuando se desee confeccionar solicitudes de valoración parcial de documentos.*

*h) Asistir junto con el superior jerárquico o quien este delegue, a las reuniones u otras actividades que convoque el Comité de Selección y Eliminación de Documentos.*

*i) Dejar constancia de los documentos eliminados mediante la confección de un acta de eliminación de documentos que deberá conservarse permanentemente en la oficina ejecutora o archivo de gestión.*

*j) Trasladar la documentación, mediante listas de remisión al Archivo Central o al Archivo Nacional (en caso de que al documento se le otorgue valor científico cultural).*

*k) Proteger la documentación de factores químicos, biológicos, físicos, materiales y ambientales, que puedan afectar su conservación. Queda prohibido mantener alimentos cerca de los archivos.*

*l) Informar al Archivo Central cualquier riesgo o desastre ocurrido en los archivos de gestión.*

*m) Conocer y aplicar el Plan de prevención y conservación de documentos ante posibles riesgos o desastres.*

*n) Solicitar asesoría técnica al Archivo Central para la restauración de cualquier documento con valor administrativo, legal, permanente e histórico.*

*o) Mantener un control de préstamo de documentos.*

*p) Otras que se deriven de la normativa vigente.*

***Artículo 7°-*** *Es obligación de las Jefaturas y Direcciones:*

*a) Informar al Archivo Central quien es la persona responsable de los archivos de gestión.*

*b) Comunicar al Archivo Central los proyectos a digitalizar o capturar y conservar los documentos de sus Archivos de Gestión.*

*Aplicar en todo proyecto para digitalizar y conservar documentos electrónicos, las Normas Técnicas emitidas por la Junta Administrativa del Archivo Nacional.*

***Artículo 9°-*** *Las funciones y deberes de las personas funcionarias del Archivo Central del MTSS, serán además de las contempladas en este artículo, las que se instruyan mediante los procedimientos e instructivos que se emitan para tal fin, y que lleve el Archivo Central.*

*a) Crear una cultura archivística en el ámbito institucional.*

*b) Capacitar a las personas funcionarias para la efectiva organización y manejo de los archivos de la institución.*

*c) Reunir el acervo documental de las dependencias y oficinas de la institución, de acuerdo con las tablas de remisión de documentos.*

*d) Coordinar la organización y administración de los archivos de gestión, periféricos y especializados por ser estas fuentes primarias de información para alimentar el Archivo Central.*

*e) Asesorar en materia archivística a las personas encargadas de los archivos de la institución.*

*f) Mantener técnicamente organizados y conservar todos los documentos institucionales.*

*g) Salvaguardar toda aquella documentación que de una u otra manera sea amenazada su integridad, por medio electrónico, así como reproducir por el mismo medio los documentos de mayor consulta.*

*h) Ejercer los controles necesarios para el adecuado manejo, seguridad y conservación de la documentación custodiada.*

*i) Velar por la aplicación de políticas archivísticas implementadas por la Junta Administrativa del Archivo Nacional y el cumplimiento de la legislación vigente en materia archivística y de la administración pública en general.*

*j) Elaborar tablas generales de plazos de conservación de documentos del Ministerio, basadas en las tablas de plazos de los archivos de gestión y someterlas a conocimiento del Comité Institucional de Selección y Eliminación de documentos.*

*k) Facilitar el acceso a la información a las personas funcionarias del Ministerio y público en general.*

*l) Observar y ayudar a las personas usuarias para que se cumplan las disposiciones de préstamos y consulta de documentos.*

*m) Conocer las nuevas técnicas archivísticas, mediante una comunicación directa con el Archivo Nacional y cualquier otro órgano competente.*

*n) Estar informado sobre materia archivística mediante capacitaciones, congresos.*

*o) Realizar un programa de limpieza anual a los documentos para su buen estado de conservación.*

*p) Presentar semestralmente informes de labores a las dependencias competentes.*

*q) El Archivo Central deberá presentar un informe anual en el mes de marzo al Archivo Nacional.*

*r) Elaborar un programa de descripción de documentos. La descripción se realizará de conformidad con las normas internacionales y nacionales vigentes.*

*s) Elaborar un plan de transferencias de los archivos de gestión al Archivo Central.*

*t) Elaborar un plan de prevención y conservación de documentos ante posibles riesgos y desastres.*

*u) Procurará contar con un programa de actividades de difusión de carácter educativo y cultural, sobre los documentos que custodian, para lo cual podrán establecer Convenios de Cooperación con archivistas de otras Instituciones, o establecer alianzas estratégicas para este fin.*

***Artículo 10.-*** *Las funciones, obligaciones y atribuciones de la persona funcionaria encargada del Archivo Central del MTSS, serán además de las contempladas en este artículo, las que se instruyan mediante los procedimientos e instructivos que se emitan para tal fin, y que lleve el Archivo Central.*

*a) Planificar, organizar, dirigir, coordinar y mantener mediante procedimientos técnicos al SIAR-MTSS.*

*b) Elaborar las normas y procedimientos para la organización del SIAR-MTSS.*

*c) Velar por que el Archivo Central disponga de los medios técnicos que faciliten su labor.*

*d) Mantener una estrecha relación con las autoridades competentes de este Ministerio con el fin de resolver aspectos administrativos y para el cumplimiento de la Ley del Sistema Nacional de Archivos y las normas que dicte el Archivo Central.*

*e) Solicitar al Comité Institucional de Selección y Eliminación de Documentos, autorización para eliminar documentos.*

*f) Evacuar consultas técnicas en materia archivística.*

*g) Mantener un sistema adecuado para el control del préstamo de documentos.*

*h) Atender consultas sobre los documentos custodiados en el Archivo Central de acuerdo con la solicitud de las personas usuarias internos o externos.*

*i) Expedir todo tipo de certificaciones y constancias, con base en los fondos documentales del Archivo Central.*

*j) Realizar como mínimo una vez al año una supervisión de los archivos periféricos, de gestión y especializados.*

k) *Denunciar y dar seguimiento ante las instancias administrativas competentes, del incumplimiento de los deberes relativos a la administración de documentos.*

*l) Denunciar y dar seguimiento, ante el Ministerio Público, de la apropiación ilegal de documentos producidos en las Instituciones Públicas y eliminación de documentos sin autorización de la Comisión Nacional de Selección y Eliminación de Documentos (CNSED), para la aplicación de lo dispuesto en los artículos 8, 9 y 36 de la Ley No. 7202 y su reglamento.*

***Artículo 16.-*** *Toda persona que consulte documentos o expedientes en el Archivo Central, debe observar las siguientes normas:*

*a) Si es funcionario activo solicitar el o los documentos por medio de formulario electrónico del Archivo Central; si es usuario externo, identificarse presentando documento idóneo, de previo a llenar la boleta de préstamo de documentos.*

*b) No doblar o arrugar los documentos.*

*c) No rayar, calcar o escribir sobre los documentos.*

*d) No comer, beber o fumar dentro del Archivo Central.*

*e) No humedecer los dedos en el momento de pasar las páginas de los documentos.*

*f) Guardar silencio durante el momento de la consulta.*

*Cuando las circunstancias lo ameriten, la persona encargada del Archivo Central podrá adicionar otras normas con la intención de salvaguardar la documentación en custodia. Estas normas se tendrán en lugar visible en el Archivo Central para la debida información de la persona usuaria.*

***Artículo 28.-*** *Los documentos que se remitan al Archivo Central serán los producidos por las diferentes dependencias del Ministerio y que hayan concluido el trámite administrativo.*

*Para tal efecto, el Archivo Central contará con un Plan de Transferencias, tanto de los archivos de gestión al Archivo Central, como de este al Archivo Nacional, con su tipología documental, series perfectamente identificadas y plazos de transferencia, según las vigencias establecidas en las tablas de plazos de conservación de documentos.*

***Artículo 30.-*** *La transferencia por parte de la oficina productora, remitirá la documentación debidamente clasificada, ordenada y acompañada por la respectiva lista de remisión electrónica y editable y otra firmada digitalmente por la Jefatura, por medio del Sistema Gestión Documental.*

***Artículo 31.-*** Además de lo establecido en el artículo anterior, la transferencia de documentos al Archivo Central, se ajustará a lo siguiente:

*a) La oficina solicitará la transferencia por escrito según Plan de Transferencias establecido por el Archivo Central.*

*b) La Jefatura del Archivo Central, autorizará y confirmará por escrito la fecha para llevar a cabo la transferencia.*

*c) Todo acervo documental que sea enviado al Archivo Central deberá contar con carátula en cada caja debidamente rotuladas e indicando su contenido.*

*d) El personal del Archivo Central confrontará con las personas funcionarias responsables de la transferencia de los documentos con sus listas de remisión.*

*e) El Archivo Central podrá aportar las cajas que la oficina considere necesarias para las transferencias en casos excepcionales. En caso de que la oficina o programa realice la compra de las cajas, deberá solicitar del Archivo Central las especificaciones técnicas de las mismas.*

***Artículo 32.-*** *AI finalizar el período de gobierno cada cuatro años, los Despachos del Ministro, Viceministros y la Unidad de Prensa realizaran una transferencia de documentos al Archivo Nacional. Para cumplir con este trabajo el Archivo Central y el Archivo Nacional asesorarán a los Despachos respectivamente.*

## *CAPÍTULO VII*

### *Archivos especializados, periféricos y/o Oficinas Regionales*

***Artículo 33.-*** *Los archivos especializados, periféricos y/o Oficinas Regionales pertenecen al SIAR-MTSS y dependen del Archivo Central para el acatamiento de políticas archivísticas y supervisión técnica.*

***Artículo 34.-*** *Es responsabilidad de las Jefaturas de los archivos especializados, periféricos y/o Oficinas Regionales nombrar a una persona encargada del archivo y a la vez comunicarlo al Archivo Central.*

***Artículo 35.-*** *Son funciones de las personas encargadas de los archivos especializados, periféricos y/o Oficinas Regionales, además de las contempladas en el artículo 4 del reglamento de la Ley No. 7202 las siguientes:*

*a) Ejecutar y coordinar con el Archivo Central las políticas archivísticas, metodológicas y técnicas.*

*b) Aplicar los instrumentos descriptivos necesarios para el debido funcionamiento y control de los documentos en estos archivos.*

*c) Garantizar la custodia, conservación, clasificación, ordenamiento, descripción y administración de la documentación.*

*d) Coordinar con el Archivo Central la confección y actualización de tablas de plazos de conservación de documentos o la confección de solicitudes de valoración parcial de documentos.*

*e) Asistir a las reuniones y otras actividades que convoque el Comité Institucional de Selección y Eliminación de Documentos y la jefatura del Archivo Central.*

*f) Dejar constancia de los documentos eliminados mediante la confección de un acta de eliminación de documentos.*

*g) Solicitar asesoría al Archivo Central sobre cualquier asunto de valor administrativo, legal, permanente e histórico de los documentos.*

*h) Comunicar e informar al Archivo Central sobre proyectos de avance tecnológico que tengan los Archivos Periféricos y Oficinas Regionales de Inspección.*

*i) Mantener los debidos controles de préstamo de documentos.*

*Cualquier otra función que se les encomiende, la cual será comunicada de manera oportuna y por los medios oficiales correspondientes.*

***Artículo 38.-** Este Comité tendrá las siguientes funciones y atribuciones; según lo establecen los artículos 22 y 23 del Reglamento a la Ley No. 7202:*

*a) Evaluar y determinar la vigencia administrativa y legal de los documentos del Ministerio.*

*b) Potestad de convocar a cualquier Departamento del MTSS para elaborar las Tablas de Plazos de Conservación y así dar valor a los diferentes tipos documentales con que cuenta el Ministerio.*

*c) Someter a la aprobación de la Comisión Nacional de Selección y Eliminación de Documentos (CNSED), las tablas de plazos.*

*d) Someter a la aprobación de la Comisión Nacional de Selección y Eliminación de Documentos (CNSED), la determinación del valor científico, cultural, social e histórico de los documentos y demás material informativo para el Ministerio.*

*e) Consultar a la Comisión Nacional de Selección y Eliminación de Documentos (CNSED), cuando deba eliminar documentos que hayan finalizado su trámite administrativo.*

*f) Conocer y aplicar las Resoluciones emitidas por la Comisión Nacional de Selección y Eliminación de Documentos (CNSED).*

***Artículo 41.-*** *Cuando las personas funcionarias de este Ministerio, no efectúen la devolución de documentos o expedientes al vencimiento del plazo conferido, el Archivo Central procederá a solicitarle por escrito la entrega de los mismos dentro de los siguientes tres días hábiles. Vencido el término anterior sin que el funcionario/a haga entrega de la documentación facilitada, el Archivo Central le informará a los superiores de éste, para que se proceda conforme indican los artículos 12 inciso k), 122 inciso b) y 124 inciso a) del Reglamento Autónomo de Servicio, Decreto Ejecutivo No. 27969-MTSS, del 23 de junio de 1999.*

***Artículo 42.-*** *Cuando la persona funcionaria no devuelva definitivamente el documento, al vencimiento del término anterior, el Archivo Central le informará a los superiores de éste y formulará las denuncias administrativas o judiciales correspondientes, según los incisos k y l) del artículo 10 de este Reglamento; 37, 38 y 97 del Reglamento a la Ley No.*

*7202; para que se proceda conforme indican los artículos 12 inciso k) y 120 del Reglamento Autónomo de Servicio del Ministerio de Trabajo y Seguridad Social y 8 y 9 de la Ley No. 7202 del Sistema Nacional de Archivos, según corresponda.*

***Artículo 44.-*** *Uso del correo electrónico. La información enviada y recibida por correo electrónico se utilizará para agilizar los trámites administrativos y deberán remitirse de forma escrita en el momento oportuno para que así este adquiera un valor administrativo legal. Los documentos públicos electrónicos, llevarán la firma digital certificada de acuerdo con la Ley de certificados, firmas digitales y documentos electrónicos y serán ingresados por los funcionarios que los reciben al Sistema de Gestión Documental del Ministerio.*

***Artículo 45.-*** *Información automatizada y digitalizada. El uso de la digitalización no implica de ninguna manera la eliminación del documento original sin la autorización correspondiente y emitida por la Comisión Nacional de Selección y Eliminación de Documentos (CNSED).*

***Artículo 49.-*** *El MTSS deberá aplicar prácticas formales para la migración de datos o transferencia de documentos electrónicos y/o información, que le permitan preservar o mantener la integridad física y funcional de dichos documentos, con el fin de asegurar la gestión adecuada de la información.*

**Artículo 2**.-Rige a partir de su publicación.

Dado en la Presidencia de la República, a los veintiséis días del mes de junio del dos mil veintitrés.

RODRIGO CHAVES ROBLES.—El Ministro de Trabajo y Seguridad Social, Andrés Romero Rodríguez.—O. C. N° 016-2023.—Solicitud N° 4600072466.—( D44182 - IN2023807127 ).

# N° 44187-MGP

EL PRESIDENTE DE LA REPÚBLICA
Y EL MINISTRO DE GOBERNACIÓN Y POLICÍA

De conformidad con lo dispuesto por los artículos 140, incisos 3) y 18) y 146 de la Constitución Política; 25, 27 inciso 1), 28, inciso 2, acápite b), de la Ley General de la Administración Pública, Ley N° 6227 del 2 de mayo de 1978 y los artículos 2, 5°, 7°, 47°, 87° inciso 1) y 90 de la Ley General de Migración y Extranjería, Ley N° 8764 del 19 de agosto de 2009 publicada en el Diario Oficial *La Gaceta* N° 170 del 01 de setiembre de 2009.

*Considerando*:

I.—Que la Ley General de Migración y Extranjería, Ley N° 8764, en su artículo 2° declara la materia migratoria de interés público para el desarrollo del país, sus instituciones y la seguridad pública.

II.—Que el artículo 47 de la Ley General de Migración y Extranjería regula la potestad de establecer las directrices generales de visas de ingreso y permanencia para no residentes en el país.

III.—Que la Ley General de Migración y Extranjería no regula expresamente el plazo máximo durante el cual una persona extranjera pueda permanecer de manera regular en el país, bajo la subcategoría de turismo,

IV.—Que por criterios de mérito, oportunidad y conveniencia, y en virtud de que el turismo es una de las principales fuentes de ingreso a nivel nacional y que los visitantes cuyes nacionalidades se encuentran dentro del primer grupo de ingreso de las Directrices Generales de Visas de Ingreso y Permanencia para No Residentes, son los que mayor cantidad de recursos generan al país, y por ende contribuyen positivamente en la reactivación de la economía nacional, según la base de datos de movimientos migratorios de la Dirección General de Migración y Extranjería, por lo que, se considera pertinente determinar un período ampliado de permanencia de este grupo, con la finalidad de que puedan mantenerse más tiempo en el país de forma regular como no residentes, subcategoría turismo.

V.—Que de conformidad con la Ley Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Ley N° 8220 del 4 de marzo de 2002 y el artículo 12 bis del Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos, Decreto Ejecutivo N° 37045-MP-MEIC del 22 de febrero de 2012, se determina que la presente regulación no establece ni modifica trámites, requisitos o procedimientos que la persona administrada debe cumplir ante la Administración Central. **Por tanto**,

DECRETAN

"MODIFICACIÓN AL DECRETO EJECUTIVO N°36626-G, DEL 23 DE MAYO DEL 2011, DENOMINADO REGLAMENTO PARA EL OTORGAMIENTO DE VISAS DE INGRESO A COSTA RICA Y AL DECRETO EJECUTIVO N° 37112-G DEL 21 DE MARZO DE 2012, DENOMINADO REGLAMENTO DE EXTRANJERÍA Y CRÉA DÍA DEL COSTARRICENSE EN EL EXTERIOR, CUYA FECHA DE CONMEMORACIÓN SERÁ EL 11 DE ABRIL DE CADA AÑO"

Artículo 1º—Modifíquese el párrafo primero y el inciso 1) del artículo 7 del Reglamento para el Otorgamiento de Visas de ingreso a Costa Rica, Decreto Ejecutivo N° 36626-G del 23 de mayo de 2011, publicado en el Diario Oficial *La Gaceta* N° 118 del 20 de junio de 2011, para que se lea de la siguiente forma:

*"Artículo 7º—Las Directrices Generales de Visas de Ingreso y Permanencia para No Residentes en el país, dividirán los diferentes países del mundo en cuatro grupos:*

*1. En el primer grupo se ubicarán los países cuyos nacionales podrán ingresar sin necesidad de requerir visa. El plazo máximo de permanencia legal para las personas extranjeras cuyas nacionalidades se ubiquen dentro de este grupo, será el que determine el funcionario de la Dirección General competente para realizar el control de entrada al país, que en ningún caso podrá ser mayor de ciento ochenta días naturales contados a partir de su ingreso".*

Artículo 2º—Modifíquese el artículo 8 del Reglamento para el Otorgamiento de Visas de ingreso a Costa Rica, Decreto Ejecutivo N° 36626-G del 23 de mayo de 2011, publicado en el Diario Oficial *La Gaceta* N° 118 del 20 de junio de 2011, para que en lo sucesivo se lea de la siguiente manera:

*"Artículo 8º—Se considerarán como "No Residentes", las personas extranjeras a quienes la Dirección General les otorgue autorización de ingreso y permanencia por un plazo que no podrá exceder los ciento ochenta días naturales, para el caso de los nacionales de países ubicados en el primer grupo de ingreso; y hasta treinta días naturales, en el caso de las nacionalidades que conforman los tres grupos restantes de las Directrices Generales de Visas de Ingreso y Permanencia para No Residentes en el país, dictadas por la Dirección General de Migración y Extranjería de conformidad con los artículos 47y 48 de la Ley 7 del presente Reglamento.*

Artículo 3º—Modifíquese el artículo 156 del Reglamento de Extranjería y Crea Día del Costarricense en el Exterior, cuya fecha de conmemoración será el 11 de abril de cada año, Decreto Ejecutivo N° 37112-G del 21 de marzo de 2012, publicado en el Alcance N° 64, a *La Gaceta* N° 95, del 17 de mayo del 2012:

*"Articulo 156.-Las personas extranjeras que hayan ingresado legalmente al país bajo la subcategoría migratoria de Turismo, y se les haya autorizada menos de noventa días de permanencia, podrán por una única vez, solicitar una prórroga de turismo, hasta alcanzar un máximo de ese plazo. A las personas a quienes se les haya autorizado un periodo de Turismo por noventa días o más, no lo podrán prorrogar."*

Artículo 4º—Este decreto ejecutivo empieza a regir ocho días naturales después de su publicación.

Dado en la Presidencia de la República, San José, a los 15 días del mes de junio del dos mil veintitrés.

RODRIGO CHAVES ROBLES.—El Ministro de Gobernación y Policía, Mario Zamora Cordero.—1 vez.—O.C.Nº 4600075779.—Solicitud Nº 013-DAF.—( D44187 - IN2023807274 ).

# REGLAMENTOS

## JUNTA DE PROTECCIÓN SOCIAL

### Gerencia de Producción, Comercialización y Operaciones

**REGLAMENTO PARA EL JUEGO NUEVOS TIEMPOS**

Artículo 1º—Para los efectos de la presente reglamentación, se entiende por:

**Apuesta:** Disposición por parte del jugador de una cierta suma de dinero para participar en un sorteo específico, con la posibilidad de obtener un premio.

**Apuesta con Reventados:** modalidad de juego de Nuevos Tiempos donde hay disposición por parte del jugador de una cierta suma de dinero para participar en un sorteo específico, adicional a la apuesta de Nuevos Tiempos; donde si el jugador selecciona esta opción, tiene la posibilidad de obtener un premio adicional.

**Apuesta con Mega Reventados:** modalidad de juego de Nuevos Tiempos donde hay disposición por parte del jugador de una cierta suma de dinero para participar en un sorteo específico, adicional a la apuesta de Nuevos Tiempos Reventados; donde si el jugador selecciona esta opción, tiene la posibilidad de obtener un premio adicional.

**Comprobante de transacción:** Tiquete impreso por una terminal ubicada en un punto de venta autorizado en donde se indican las características de las apuestas o pago de premios realizados al jugador, incluyendo, pero no limitado a, nombre del producto comprado, monto en dinero apostado, números seleccionados por el jugador, fechas, número de sorteo, entre otros.

**Gallo tapado:** Apuestas que el sistema emite de manera aleatoria.

**Hora de cierre de apuestas:** Se refiere al momento en que se cierra la recepción de apuestas para un sorteo en particular.

**Jugada multi-sorteos:** El jugador tendrá la oportunidad de hacer apuestas a sorteos consecutivos que se realicen al mediodía, en la tarde, en la noche o a cualquier hora del día, hasta un límite de 10 sorteos incluyendo el vigente.

**Jugadas en avance:** Apuestas en sorteos que ocurrirán en el futuro, a partir de un sorteo que ocurre después del próximo, que se realicen al mediodía, en la tarde, en la noche o a cualquier hora del día, siempre y cuando la apuesta se realice para uno de los sorteos contenidos en los siguientes 8 días naturales contados a partir del momento de la compra.

**Jugadas multi-sorteo en avance:** Apuestas multi-sorteo (10 sorteos) en avance (a futuro), siempre y cuando el primer sorteo seleccionado de esa compra, esté contenido en uno de los siguientes 8 días naturales contados a partir del momento de la compra.

**Junta:** Junta de Protección Social.

**Jugador:** Persona mayor de edad que realiza una apuesta.

**Promoción:** Otorgamiento de premios especiales en especie, en efectivo o ambas, según corresponda, adicionales y asociados con el Juego Nuevos Tiempos y sus modalidades, por un período determinado, con la finalidad de incentivar la venta del producto.

**Punto de venta:** Personas físicas o jurídicas autorizados por la Junta para la venta y pago de premios al público de los productos de apuestas. Sitio o persona que cuenta físicamente con una o más terminales del sistema especializado para la venta de lotería electrónica.

**Premio fijo:** Premio que asegura a los ganadores un monto de dinero fijo sin importar la cantidad de ganadores.

**Sorteo:** Proceso de selección al azar que determina la combinación ganadora de un premio, realizado y fiscalizado de acuerdo con lo establecido en el Reglamento a la Ley de Loterías, en el Reglamento interno para regular las actividades relacionadas con la realización y la asistencia a la celebración de los sorteos de lotería y a la recepción de excedentes de loterías, así como cualquier otra normativa que se emita al efecto.

**Sistema:** Software en línea y tiempo real que administra cada una de las transacciones producto de la venta de lotería electrónica o procesamiento transaccional del pago de premios.

**Transacción:** Operación procesada enteramente de una sola vez, recibiendo un identificador (número serial) único en el sistema.

**Terminal:** Dispositivo de entrada y salida remoto de datos, producción de documentos impresos y comunicación de mensajes originados en un sistema remoto de cómputo central (dispositivo físico - equipo - utilizado para la venta y procesamiento transaccional del pago de premios de lotería electrónica).

Artículo 2º—**Condiciones.** El objeto del presente Reglamento es establecer las condiciones que rigen la venta y pago de premios del juego Nuevos Tiempos en sus diferentes modalidades, la realización de promociones y la ejecución de sus sorteos, sin que suponga se concierte contrato alguno entre los jugadores, ni entre éstos y la Junta, quedando limitada la actividad de quienes participan a pagar el importe correspondiente y efectuar sus apuestas en la forma establecida por estas normas.

El hecho de realizar una apuesta implica por parte del jugador, el conocimiento de este Reglamento y la adhesión a éste, quedando sometida su apuesta a las normativas del presente Reglamento.

Artículo 3º—**Obligaciones del jugador.** El jugador es responsable de verificar, en el momento de realizar la transacción que los datos de la apuesta sean correctos conforme lo establecido en el presente Reglamento.

Artículo 4º—**Del juego denominado Nuevos Tiempos y sus modalidades.** Es un juego que consiste en diferentes modalidades de apuestas, donde el jugador puede escoger un número entre un rango de números definidos según la modalidad seleccionada y se gana cuando el número favorecido en el sorteo realizado por la Junta concuerda con el número previamente seleccionado por el jugador de acuerdo con las características descritas a continuación referente a las modalidades de juego.

**Modalidades de juego:** El juego Nuevos Tiempos incluye cinco diferentes modalidades de juego, como se describen en este reglamento, para las cuales se deben hacer apuestas independientes y su comprobante indicará la modalidad seleccionada por el jugador.

- Exacto: El jugador debe seleccionar por cada apuesta un número entre el 00 y el 99. Se gana cuando el número seleccionado concuerda con el número favorecido en el sorteo realizado por la Junta. Esta es la única modalidad del juego Nuevos Tiempos en la cual se puede jugar también la opción de Nuevos Tiempos Reventados, descrita en el presente artículo.
- Reversible: En esta modalidad de jugada, el jugador selecciona de la misma manera un número entre el 00 al 99, sin embargo, en esta modalidad el jugador tiene doble posibilidad de ganar, una manera es si obtiene el número exacto favorecido en el sorteo y la otra manera es si su número es el inverso del número favorecido. Para los números cuyo primer digito y segundo digito sean iguales (00, 11, 22, 33, 44, 55, 66, 77, 88, 99) en esta modalidad no aplica.
- Primero: En esta modalidad de jugada, el jugador apuesta por el primer dígito del número ganador del sorteo de la Junta, de manera que puede escoger un número del 0 al 9 y gana si el primer digito del número favorecido en el sorteo concuerda con el primer dígito del número apostado.
- Terminación: En esta modalidad de jugada, el jugador apuesta por el último dígito del número ganador del sorteo de la Junta, de manera que puede escoger un número del 0 al 9 y gana si el último digito del número favorecido en el sorteo concuerda con el último dígito del número apostado.
- Apuesta con Reventados: esta modalidad se juega en combinación con la modalidad Exacto y sólo se puede adquirir si el jugador compró su jugada con Exacto. El jugador invierte un monto adicional a la modalidad Exacto y con eso participa en un segundo sorteo que sucede inmediatamente después del sorteo de Nuevos Tiempos donde se seleccionó un número entre 00 y 99. Si el número seleccionado por el jugador en la modalidad de Exacto coincide con el favorecido en el sorteo de Nuevos Tiempos, el jugador gana el premio correspondiente a Exacto.
- Apuesta con Mega Reventados: esta modalidad se juega en combinación con la modalidad Reventados y sólo se puede adquirir si el jugador compró su jugada con Exacto. El jugador invierte un monto adicional a la modalidad Exacto y a la modalidad Reventados, elige un segundo número entre el 00 y el 99, que puede ser igual o diferente al elegido para la modalidad Exacto y Reventados, y participa en un tercer sorteo que sucede inmediatamente después del sorteo de Nuevos Tiempos Reventados. Si el número seleccionado por el jugador en la modalidad de Mega Reventados coincide con el favorecido en el sorteo de Nuevos Tiempos Mega Reventados, el jugador gana el premio correspondiente.

Si además sale premiada la bolita denominada Reventada en el segundo sorteo, el jugador que haya seleccionado jugar Nuevos Tiempos Reventados, gana el premio adicional. Para optar por el premio de Nuevos Tiempos Reventados, debe haber jugado y acertado la modalidad Exacto. En caso que no salga premiada la bolita denominada Reventada en el segundo sorteo, el jugador puede ser acreedor de un premio por haber efectuado una Apuesta con Mega Reventados.

Artículo 5º—**De las promociones.** Corresponde a la Junta Directiva aprobar la mecánica, el plan de premios y la vigencia de las promociones asociadas con el Juego Nuevos Tiempos.

Corresponde a la Gerencia General emitir el procedimiento de cada promoción, el cual debe ser publicado en el Diario Oficial *La Gaceta*.

Los sorteos para determinar los ganadores de las promociones se realizarán en el horario y la fecha que determine la Junta Directiva y serán fiscalizados conforme lo establecido en el artículo 75 del Reglamento a la Ley de Loterías.

El plazo para hacer efectivos los premios de las promociones, es de sesenta días naturales contados a partir del día hábil siguiente a la realización del sorteo de que se trate.

Según sea la mecánica de la promoción y los premios a otorgar, la Junta Directiva determinará si éstos se financiarán con el dos por ciento (2%) sobre las ventas brutas mensuales del Juego Nuevos Tiempos destinados a publicidad y promoción, si formarán parte del plan de premios del juego o se tomarán del fondo para premios extra.

Artículo 6º—**Estructura de premios.** El juego Nuevos Tiempos consta de una estructura de premios fijos para cada una de las modalidades, las cuales se detallan a continuación:

- **Exacto:** Paga 70 veces la inversión
- **Reversible:** Paga 35 veces la inversión
- **Primero:** Paga 7 veces la inversión
- **Terminación:** Paga 7 veces la inversión
- **Nuevos Tiempos Reventados:** paga 200 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Reventados. Estas 200 veces son independientes de las 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto. Por ende, el jugador gana 70 veces sobre la inversión específica que haya realizado en la modalidad exacto, más 200 veces sobre la inversión específica que haya realizado en Reventados, siempre y cuando se juegue y acierte la modalidad Exacto y salga premiada la bolita denominada Reventada.
- **Nuevos Tiempos Mega Reventados:**

1. Paga 2000 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue y acierte la modalidad Exacto; (ii) salga premiada la bolita denominada Reventada; y (iii) el jugador haya acertado el número de Nuevos Tiempos Mega Reventados. Estas 2000 veces son independientes de las 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto e independientes de las 200 veces que se pagan sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Reventados. Por ende, el jugador gana 70 veces sobre la inversión específica que haya realizado en la modalidad Exacto, más 200 veces sobre la inversión específica que haya realizado en Reventados, más 2000 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.
2. Paga 1000 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue y acierte la modalidad Exacto; (ii) no salga premiada la bolita denominada Reventada; y (iii) el jugador haya acertado el número de Nuevos Tiempos Mega Reventados. Estas 1000 veces son independientes de las 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto. Por ende, el jugador gana 70 veces sobre la inversión específica que haya realizado en la modalidad Exacto, más 1000 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.
3. Paga 50 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue y acierte la modalidad Exacto; (ii) salga premiada la bolita denominada Reventada; y (iii) el jugador no haya acertado el número de Nuevos Tiempos Mega Reventados. Estas 50 veces son independientes de las 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto e independientes de las 200 veces que se pagan sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Reventados. Por ende, el jugador gana 70 veces sobre la inversión específica que haya realizado en la modalidad Exacto, más 200 veces sobre la inversión específica que haya realizado en Reventados, más 50 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.
4. Paga 50 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue pero no se acierte la modalidad Exacto; (ii) salga premiada la bolita denominada Reventada; y (iii) el jugador haya acertado el número de Nuevos Tiempos Mega Reventados. Estas 50 veces son independientes de las 200 veces que se pagan sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Reventados. Por ende, el jugador gana 200 veces sobre la inversión específica que haya realizado en Reventados, más 50 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.
5. Paga 10 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue y acierte la modalidad Exacto; (ii) no salga premiada la bolita denominada Reventada; y (iii) el jugador no haya acertado el número de Nuevos Tiempos Mega Reventados. Estas 10 veces son independientes de 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto. Por ende, el jugador gana 70 veces que se pagan sobre la inversión que se haya realizado en la modalidad Exacto, más 10 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.

6. Paga 10 veces sobre la inversión específica que el jugador haya decidido adicionar para Nuevos Tiempos Mega Reventados, siempre y cuando: (i) se juegue pero no acierte la modalidad Exacto; (ii) no salga premiada la bolita denominada Reventada; y (iii) el jugador haya acertado el número de Nuevos Tiempos Mega Reventados. Por ende, el jugador gana 10 veces sobre la inversión que se haya realizado en la modalidad Nuevos Tiempos Mega Reventados, siempre y cuando se cumplan las condiciones indicadas.

Artículo 7º—**Captura de apuestas.** Los jugadores solicitarán sus apuestas pidiendo directamente al operador de la terminal en línea su introducción. El único comprobante válido es el tiquete impreso por la terminal en el punto de venta autorizado.

Otra opción que el jugador tendrá disponible es hacer su jugada con la modalidad automática o "Gallo Tapado", donde el sistema le emite una jugada con un número al azar completamente aleatorio.

Cuando el jugador realice la jugada por medio de la modalidad automática o "Gallo Tapado", en el tiquete impreso por la terminal en el punto de venta autorizado, la línea del número que se realice bajo esta modalidad debe estar acompañada de las siglas "GT" que significan "Gallo Tapado".

El monto mínimo de las apuestas para las jugadas de Nuevos Tiempos es de ₡100 (cien colones) y el jugador tiene la oportunidad de apostar por encima de este monto en múltiplos de ₡100 (cien colones) hasta un máximo de ₡50.000 (cincuenta mil colones) por apuesta.

En un mismo comprobante de transacción puede haber varias apuestas, sin embargo, la sumatoria máxima de estas apuestas no puede superar los ₡2.000.000 (dos millones de colones). La Junta se reserva, por condiciones de oportunidad en el juego, la potestad de modificar el precio de las apuestas, comunicándolo de manera oportuna.

El juego permite a los jugadores realizar jugadas multi-sorteo, jugadas en avance y jugadas multi-sorteo en avance, según las definiciones establecidas en el artículo 1.

En el caso de la modalidad de Nuevos Tiempos Reventados, el jugador tiene la oportunidad de invertir un monto adicional al que destinó a la modalidad de Exacto, que deberá ser igual o menor a la inversión efectuada para la modalidad Exacto, en múltiplos de ₡100 (cien colones) y hasta un máximo equivalente al monto apostado en la jugada de Nuevos Tiempos en su modalidad Exacto.

En el caso de la modalidad de Nuevos Tiempos Mega Reventados, el jugador tiene la oportunidad de invertir un monto adicional al que destinó a la modalidad de Nuevos Tiempos Reventados, que deberá ser igual o menor a la inversión efectuada para Nuevos Tiempos Reventados, en múltiplos de ₡100 (cien colones) y hasta un máximo equivalente al monto apostado en la jugada de Nuevos Tiempos en su modalidad Nuevos Tiempos Reventados.

En el caso de que en un mismo comprobante de transacción existan apuestas para sorteos en distintas fechas, el plazo para hacer efectivos los premios, es de sesenta días naturales contados a partir del día hábil siguiente al sorteo. Es decir, cada apuesta registrada en ese comprobante de transacción tiene distintos plazos para hacer efectivos los premios. Los días se contarán como se explica en este reglamento.

Artículo 8º—**Tiempo límite para la recepción de apuestas.** La recepción de apuestas para cada juego se inicia a partir del momento en que la Junta lo defina en el sistema automatizado. La hora de cierre o momento en que se cierra la recepción de apuestas en cada juego, será, mínimo de 15 minutos antes de la hora fijada para el inicio de dicho sorteo.

Artículo 9º—**Validación de apuestas.** Para participar en el respectivo sorteo, cada apuesta debe estar válidamente registrada en el sistema, bajo las diferentes modalidades indicadas para la captura de apuestas. Para efectos de control, cada apuesta registrada tendrá asignado un número de transacción que la identifica dentro del sistema. Para reclamar su premio debe presentar su comprobante de apuesta en perfectas condiciones y sin ningún tipo de deterioro.

Artículo 10.—**De los días de sorteos.** Los sorteos de Nuevos Tiempos y sus modalidades se realizarán los días, en el horario y la frecuencia, que determine el Calendario de Sorteos aprobado por la Junta Directiva, en las instalaciones de la Junta o en el lugar que ésta defina.

El Calendario de Sorteos para Nuevos Tiempos será publicado en los medios oficiales para conocimiento de los jugadores.

El día, la hora o el lugar de realización de estos sorteos podrán ser modificados por la Junta Directiva, previa comunicación al público general por los medios correspondientes según la Ley. Así mismo se reserva el derecho de eliminar o suprimir sorteos, siempre y cuando existan razones de fuerza mayor o caso fortuito que impidan su realización.

En caso de anticipar o suprimir el sorteo, la comunicación debe hacerse con al menos 2 días hábiles de anticipación a la fecha señalada para celebrar el sorteo, siempre y cuando no se hayan capturado apuestas para el caso de supresión del sorteo y en caso de posposición, la comunicación podrá hacerse con no menos de un día hábil de anticipación a la fecha original.

Los sorteos serán realizados y fiscalizados de acuerdo con lo establecido en el Reglamento a la Ley de Loterías, en el Reglamento interno para regular las actividades relacionadas con la realización y la asistencia a la celebración de los sorteos de lotería y a la recepción de excedentes de loterías, así como cualquier otra normativa que se emita al efecto.

Artículo 11.—**Metodología para la realización de los sorteos.** Los sorteos de Nuevos Tiempos y sus modalidades se realizarán en los días, en el horario y la frecuencia que determine el Calendario de Sorteos.

Cada sorteo del día se llevará a cabo de la siguiente manera:

Se realizará por medio de extracción de bolitas que conformen un número del 00 al 99 por medio de las tómbolas de aire o tómbolas manuales.

Posterior a este sorteo, se realiza de forma inmediata un sorteo para determinar si hay ganadores de Nuevos Tiempos Reventados. En dicha tómbola se encuentran tres bolitas donde una es premiada (denominada Reventada) y otras dos están en blanco simbolizando que no están premiadas. En el sorteo se extrae una de las tres bolitas por medio de tómbolas de aire o manuales para determinar si sale favorecida la bolita denominada Reventada.

Posterior al sorteo de Nuevos Tiempos Reventados, se realiza de forma inmediata un sorteo para determinar si hay ganadores de Nuevos Tiempos Mega Reventados. Se realizará por medio de extracción de bolitas que conformen un número del 00 al 99 por medio de las tómbolas de aire o tómbolas manuales.

En los días que se realice únicamente sorteos de Nuevos Tiempos se realizará por medio de extracción de bolitas que conformen un número del 00 al 99 por medio de las tómbolas de aire o tómbolas manuales.

Cuando estos se jueguen en combinación con los sorteos de la Lotería Popular o Lotería Nacional, el número que se tomará como favorecido para el juego de Nuevos Tiempos será el mismo número favorecido como Premio Mayor en el sorteo de Lotería Popular o Lotería Nacional correspondiente a esos días.

Luego de la realización del sorteo se procede a incluir la información por parte de los funcionarios designados para tal efecto en los sistemas respectivos. Posteriormente se elabora y firma el acta respectiva donde se oficializa el resultado del sorteo y se cargan los datos necesarios para proceder generar los pagos de los premios correspondientes.

Artículo 12.—**Pago de premios.** Los premios serán pagados al portador del comprobante de la apuesta, en los puntos de venta. En caso de que el punto de venta no tenga a su disposición suficiente dinero para cancelar el premio, el jugador podrá llamar al número del Centro de Servicio al Cliente que sea dispuesto para tales efectos, para que se le indique donde puede hacer efectivo su premio. Los requisitos para hacer efectivo un premio son presentar el comprobante de apuesta en perfectas condiciones y sin ningún tipo de deterioro y un documento de identificación vigente (cédula de identidad, cédula de residencia o pasaporte). La Junta se reserva el derecho de solicitar cualquier otra información que sea necesaria para llevar a cabo el cambio de premios mayores o iguales a USD 10.000 (diez mil dólares estadounidenses).

En caso que el comprobante de la apuesta presentase un daño físico, el jugador deberá llamar al centro de servicio al cliente respectivo al 4100-2300 para coordinar lugar, fecha y hora donde podrá presentar dicho comprobante a la Junta o a quién esta designe, en cuyo caso esta última o quién se designe podrá revisar si con los datos que quedaron sin daño es suficiente para poder realizar el pago. En caso que el daño no lo permita, el pago del premio no se podrá realizar. El jugador es responsable de cuidar como buen padre el tiquete comprado.

En caso de extravío del comprobante de la apuesta, no existirá manera de hacer efectivo el cambio de premio.

Artículo 13.—**Plazo para hacer efectivos los premios.** El plazo para hacer efectivos los premios, es de sesenta días naturales contados a partir del día hábil siguiente a la realización del sorteo.

En el caso de que en un mismo comprobante de transacción existan apuestas para sorteos en distintas fechas, el plazo para hacer efectivos los premios, es de sesenta días naturales contados a partir del día hábil siguiente a la realización del sorteo correspondiente. Es decir, cada apuesta registrada en ese comprobante de transacción tendría distintos plazos para hacer efectivos los premios. Si el plazo se computa en un día inhábil el premio se hará efectivo el día hábil inmediato siguiente.

Artículo 14.—**Premios no cambiados.** Los premios disponibles en cada sorteo que no hayan sido cambiados al finalizar el plazo para hacer efectivos los premios, se consideran parte de las utilidades del juego.

Artículo 15.—**Término para reclamos.** En caso de que exista disconformidad por parte de algún jugador sobre el pago o no de un premio o sobre el monto respectivo que se haya pagado, se podrá presentar el respectivo reclamo, el cual debe dirigirse a la Unidad de Pago de Premios, como responsable de resolver los reclamos de premios.

La fecha límite para su presentación, lo es dentro del plazo de sesenta días naturales contados a partir del día hábil siguiente al día del sorteo. La Unidad de Pago de Premios, atenderá, resolverá y comunicará al interesado su resolución, dentro del plazo de 30 días naturales al recibido de la solicitud firmada por el reclamante.

Artículo 16.—**Derogatoria.** Se deroga el "Reglamento para el Juego Nuevos Tiempos", publicado en el Alcance N° 57 a *La Gaceta* N° 52 del 17 de marzo del 2022 y sus reformas El presente Reglamento rige a partir de su publicación en el Diario Oficial *La Gaceta*.

Aprobado con el acuerdo JD-408 correspondiente al Capítulo VI), artículo 15) de la sesión ordinaria, celebrada el 24 de agosto de 2023.

Luis Fernando Madrigal Gómez, Gerente.—1 vez.—O.C.Nº 25735.—Solicitud Nº 456661.—( IN2023807314 ).