Año IV, n° 351, (28 de junio de 2021)

Legislación Oficial Actualizada Nacional

Dirección Servicios Legislativos

Biblioteca del Congreso
ARGENTINA

Presentación

La Dirección Servicios Legislativos de la Biblioteca del Congreso de la Nación brinda, a través de la presente publicación de entrega diaria, una selección de normas trascendentes de carácter general, con la intención de garantizar al lector el acceso a la información oficial cierta.

A tal fin contiene una breve referencia de la norma seleccionada y a continuación el texto completo de la misma tal y como fue publicada en el Boletín Oficial de la República Argentina.

Índice

Legislación

- Prohíbe hasta el 31 de diciembre de 2021, efectuar despidos y/o suspensiones sin justa causa y por las causales de falta o disminución de trabajo y fuerza mayor, en virtud de la emergencia pública por la pandemia por Covid-19.

  Decreto de Necesidad y Urgencia N° 413 (25 de junio de 2021).
  Publicado: Boletín Oficial de la República Argentina 28 de junio de 2021. Páginas 3 - 5.

- Aprueba los "Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional", con el fin de prevenir que sus sistemas de información se vean afectados. La presente medida se aplicará a las entidades del sector Público Nacional, comprendidas en la ley 24156 de Administración Financiera.

  Decisión Administrativa N° 641 Jefatura de Gabinete de Ministros (25 de junio de 2021).
  Publicado: Boletín Oficial de la República Argentina 28 de junio de 2021. Páginas 8 - 11.

- Establece que las y los titulares de cada jurisdicción, organismo o entidad comprendido en el artículo 8° de la Ley N° 24.156 y sus modificatorios, podrán convocar al retorno a la actividad laboral presencial a las y los trabajadores que hubieren recibido al menos la primera dosis de cualquiera de las vacunas destinadas a generar inmunidad adquirida contra el COVID-19 autorizadas para su uso en la República Argentina, independientemente de la edad y la condición de riesgo, transcurridos catorce (14) días de la inoculación. Establece condiciones para personal de la salud, y para personas que no quieran vacunarse.

  Resolución N° 62 Secretaría de Gestión y Empleo Público (25 de junio de 2021).
  Publicado: Boletín Oficial de la República Argentina 28 de junio de 2021. Páginas 27 - 29.

- Crea el Programa "Becas País Digital" con el objeto de fomentar la inclusión digital y la participación de mujeres y diversidades en la industria de las Tecnologías de la Información y las Comunicaciones (TIC) y de capacitar en programación, marketing digital y ciencia de datos, a fin de responder a la demanda laboral de personas calificadas en habilidades digitales.

  Resolución N° 65 Secretaría de Innovación Pública (24 de junio de 2021).
  Publicado: Boletín Oficial de la República Argentina 28 de junio de 2021. Páginas 32 - 33.

- Crea el Programa "Sumar Capacitación" con el objetivo principal de fortalecer la libertad de expresión, generando una mayor pluralidad cultural e informativa mediante la formación de los actores vinculados a los medios de gestión social de la República Argentina.

  Resolución N° 9618 Secretaría de Medios y Comunicación Pública (24 de junio de 2021).
  Publicado: Boletín Oficial de la República Argentina 28 de junio de 2021. Páginas 34 - 36.

Textos Oficiales

- Decreto de Necesidad y Urgencia N° 413
  (25 de junio de 2021)

- Decisión Administrativa N° 641 Jefatura de Gabinete de Ministros
  (25 de junio de 2021)

- Resolución N° 62 Secretaría de Gestión y Empleo Público
  (25 de junio de 2021)

- Resolución N° 65 Secretaría de Innovación Pública
  (24 de junio de 2021)

- Resolución N° 9618 Secretaría de Medios y Comunicación Pública
  (24 de junio de 2021)

EMERGENCIA PÚBLICA EN MATERIA OCUPACIONAL

Decreto 413/2021

DECNU-2021-413-APN-PTE - Prohibiciones de despidos y suspensiones. Prórroga.

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente N° EX-2021-54490896-APN-DGD#MT, la Ley N° 27.541, los Decretos Nros. 34 del 13 de diciembre de 2019, 156 del 14 de febrero de 2020, 260 del 12 de marzo de 2020, 297 del 19 de marzo de 2020, 329 del 31 de marzo de 2020, 367 del 13 de abril de 2020, 487 del 18 de mayo de 2020, 528 del 9 de junio de 2020, 624 del 28 de julio de 2020, 761 del 23 de septiembre de 2020, 891 del 13 de noviembre de 2020, 961 del 29 de noviembre de 2020, 39 del 22 de enero de 2021, 235 del 8 de abril de 2021, 266 del 21 de abril de 2021, 287 del 30 de abril de 2021, 334 del 21 de mayo de 2021, 345 del 27 de mayo de 2021 y 381 del 11 de junio de 2021, su respectiva normativa modificatoria y complementaria, y

CONSIDERANDO:

Que mediante el Decreto N° 34/19 se declaró la emergencia pública en materia ocupacional, la que fue ampliada por los Decretos N° 528/20, N° 961/20 y N° 39/21, hasta el 31 de diciembre de 2021.

Que por la Ley N° 27.541 se declaró la emergencia pública en materia económica, financiera, fiscal, administrativa, previsional, tarifaria, energética, sanitaria y social, la que posteriormente se dispuso ampliar en materia sanitaria a través del Decreto N° 260/20, en virtud de la pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con la COVID-19, por el plazo de UN (1) año; el que como consecuencia del agravamiento de la situación epidemiológica, fue prorrogado por el Decreto N° 167/21, hasta el 31 de diciembre de 2021.

Que, oportunamente, para hacer frente a la citada emergencia, a través del Decreto N° 297/20 se dispuso el “aislamiento social, preventivo y obligatorio” (ASPO), durante el plazo comprendido entre el 20 y el 31 de marzo de 2020, el que fue sucesivamente prorrogado mediante los Decretos Nros. 325/20, 355/20, 408/20, 459/20 y 493/20.

Que, posteriormente, por los Decretos Nros. 520/20, 576/20, 605/20, 641/20, 677/20, 714/20, 754/20, 792/20, 814/20, 875/20, 956/20, 1033/20, 67/21, 125/21 y 168/21 -cuya vigencia fue dejada sin efecto a partir del 9 de abril de 2021 por el Decreto N° 235/21- se fue diferenciando a las distintas áreas geográficas del país, entre aquellas que pasaron a una etapa de “distanciamiento social, preventivo y obligatorio” (DISPO) y aquellas que debieron retornar a la etapa de ASPO, en virtud de la evolución de la pandemia y de acuerdo al estatus sanitario de cada provincia, departamento y aglomerado, por sucesivos períodos.

Que luego, mediante los Decretos Nros. 235/21 y su modificatorio 241/21, y 287/21, prorrogado por sus similares Nros. 334/21 y 381/21, se establecieron medidas generales de prevención y disposiciones locales y focalizadas de contención, basadas en evidencia científica y en la dinámica epidemiológica, que deben cumplir todas las personas,

con el fin de mitigar la propagación del virus SARS-CoV-2 y su impacto sanitario, hasta el 25 de junio de 2021, inclusive.

Que, como se ha señalado reiteradamente, en el contexto descripto el Estado Nacional ha adoptado medidas de contención que tienen como objetivo ayudar a las empresas a sobrellevar los efectos de la emergencia, dictando como correlato necesario a las medidas de apoyo y sostén para el funcionamiento de las mismas medidas de tutela y protección de los puestos de trabajo, a través de los Decretos Nros. 329/20, 487/20, 624/20, 761/20, 891/20, 39/21, 266/21 y 345/21.

Que la segunda ola de COVID-19 que azota al país debe ser acompañada por medidas acordes que contemplen la protección de la salud de la población y coadyuven a morigerar el impacto de las medidas sanitarias sobre el empleo.

Que mediante el Mensaje N° 48 del 10 de mayo de 2021, el PODER EJECUTIVO NACIONAL envió al HONORABLE CONGRESO DE LA NACIÓN un Proyecto de Ley por el cual se proponen indicadores precisos para establecer el nivel de riesgo epidemiológico y sanitario de cada zona del país, con el fin de establecer un modelo que otorgue previsibilidad al determinar las acciones y medidas que regirán ante el riesgo creciente.

Que la protección preferente de las trabajadoras y los trabajadores es una garantía que la CONSTITUCIÓN NACIONAL incluye en el artículo 14 bis y que, en idéntico sentido, normas internacionales incorporadas en el artículo 75, inciso 22, obligan a adoptar medidas robustas de mayor intensidad en contextos excepcionales que ponen en riesgo el propio tejido del sistema de relaciones laborales.

Que, en función de ello, es necesario acompañar las medidas de emergencia prorrogando la adopción de aquellas que resguardan los puestos de trabajo, como herramientas de política laboral necesarias para la protección de las trabajadoras y los trabajadores, asegurándoles que esta crisis excepcional no les hará perder sus puestos de trabajo.

Que la ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (O.I.T.) ha emitido un documento denominado “Las normas de la OIT y la COVID-19 (coronavirus)” que revela la preocupación mundial y alude a la necesidad de que los gobiernos implementen medidas dirigidas a paliar los efectos nocivos en el mundo del trabajo, en particular en lo referido a la conservación de los puestos de labor y en tal sentido recuerda la importancia de tener presente la Recomendación 166, que subraya “que todas las partes interesadas deberían tratar de evitar o limitar en todo lo posible la terminación de la relación de trabajo por motivos económicos, tecnológicos, estructurales o análogos, sin perjuicio para el funcionamiento eficaz de la empresa, establecimiento o servicio, y esforzarse por atenuar las consecuencias adversas de toda terminación de la relación de trabajo por estos motivos, para el trabajador o los trabajadores interesados”.

Que, asimismo, el mencionado organismo ha llevado a cabo un análisis pormenorizado sobre las disposiciones fundamentales de las normas internacionales del trabajo pertinentes en el contexto del brote de la COVID-19, publicado el 27 de marzo de 2020, sosteniendo que las patologías contraídas por exposición en el trabajo a dicho agente patógeno podrían considerarse como enfermedades profesionales.

Que, en ese marco, diversos países han declarado que la afección por la COVID-19 producida por la exposición de los trabajadores y las trabajadoras al virus SARS-CoV-2 durante la realización de sus tareas laborales, reviste carácter de enfermedad profesional.

Que en nuestro país, mediante el artículo 6º del Decreto Nº 345/21 se prorrogó hasta el 30 de junio de 2021, inclusive, lo dispuesto por el artículo 7° del Decreto Nº 39/21 -por el cual se estableció que por un plazo determinado la enfermedad COVID-19 producida por el virus SARS-CoV-2 será considerada presuntivamente una enfermedad de carácter profesional (no listada)-, respecto de la totalidad de las trabajadoras y los trabajadores dependientes incluidas e incluidos en el ámbito de aplicación personal de la Ley N° 24.557 sobre Riesgos del Trabajo que hayan prestado efectivamente tareas en sus lugares de trabajo.

Que subsistiendo las causas que motivaron aquella medida, corresponde prorrogar los términos de la misma.

Que las medidas que se establecen en el presente decreto son razonables y proporcionadas con relación a la amenaza y al riesgo sanitario que enfrenta nuestro país y se adoptan en forma temporaria, toda vez que resultan perentorias y necesarias para proteger la salud de determinados sectores de la población trabajadora particularmente vulnerable.

Que la Ley N° 26.122 regula el trámite y los alcances de la intervención del HONORABLE CONGRESO DE LA NACIÓN respecto de los Decretos de Necesidad y Urgencia dictados por el PODER EJECUTIVO NACIONAL en virtud de lo dispuesto por el artículo 99, inciso 3 de la CONSTITUCIÓN NACIONAL.

Que la citada ley determina que la COMISIÓN BICAMERAL PERMANENTE tiene competencia para pronunciarse respecto de la validez o invalidez de los Decretos de Necesidad y Urgencia, así como para elevar el dictamen al plenario de cada Cámara para su expreso tratamiento, en el plazo de DIEZ (10) días hábiles.

Que el artículo 22 de la Ley N° 26.122 dispone que las Cámaras se pronuncien mediante sendas resoluciones, y que el rechazo o aprobación de los decretos deberá ser expreso conforme lo establecido en el artículo 82 de la Carta Magna.

Que ha tomado intervención el servicio jurídico competente.

Que la presente medida se dicta en uso de las atribuciones conferidas por el artículo 99, incisos 1 y 3 de la CONSTITUCIÓN NACIONAL.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA EN ACUERDO GENERAL DE MINISTROS

DECRETA:

ARTÍCULO 1°.- El presente decreto se dicta en el marco de la emergencia pública en materia sanitaria declarada por la Ley N° 27.541, ampliada por el Decreto N° 260/20, sus modificatorios y su prórroga establecida por el Decreto N° 167/21 y la emergencia pública en materia ocupacional declarada por el Decreto Nº 34/19 y ampliada

por sus similares Nros. 528/20, 961/20 y 39/21.

ARTÍCULO 2°.- Prorrógase hasta el 31 de diciembre de 2021 inclusive, la prohibición de efectuar despidos sin justa causa y por las causales de falta o disminución de trabajo y fuerza mayor, dispuesta por el artículo 2° del Decreto N° 329/20 y sus sucesivas prórrogas.

ARTÍCULO 3°.- Prorrógase hasta el 31 de diciembre de 2021, inclusive, la prohibición de efectuar suspensiones por las causales de fuerza mayor o falta o disminución de trabajo, dispuesta por el artículo 3° del Decreto N° 329/20 y sus sucesivas prórrogas.

Quedan exceptuadas de esta prohibición y de los límites temporales previstos por los artículos 220, 221 y 222 de la Ley de Contrato de Trabajo N° 20.744 (t.o. 1976) y sus modificatorias, las suspensiones efectuadas en los términos del artículo 223 bis de la misma, como consecuencia de la emergencia sanitaria.

ARTÍCULO 4°.- Los despidos y las suspensiones que se dispongan en violación de lo dispuesto en el artículo 2° y en el primer párrafo del artículo 3º del presente decreto, no producirán efecto alguno y se mantendrán vigentes las relaciones laborales existentes y sus condiciones actuales.

ARTÍCULO 5°.- Las prohibiciones previstas en el presente decreto no serán aplicables a las contrataciones celebradas con posterioridad a la entrada en vigencia del Decreto N° 34/19, ni respecto del personal que preste servicios en el ámbito del Sector Público Nacional definido en el artículo 8° de la Ley N° 24.156 y sus modificatorias, con independencia del régimen jurídico al que se encuentre sujeto y de la naturaleza jurídica de la entidad empleadora.

Quedan asimismo exceptuados y/o exceptuadas de tales prohibiciones, quienes se encuentren comprendidos y/o comprendidas en el régimen legal de trabajo para el personal de la industria de la construcción regulado por la Ley Nº 22.250.

ARTÍCULO 6º.- Prorrógase hasta el 31 de diciembre de 2021, inclusive, lo dispuesto por el artículo 7° del Decreto Nº 39/21 prorrogado por el artículo 6º del Decreto Nº 345/21, respecto de la totalidad de las trabajadoras y los trabajadores dependientes incluidas e incluidos en el ámbito de aplicación personal de la Ley N° 24.557 sobre Riesgos del Trabajo y que hayan prestado efectivamente tareas en sus lugares habituales, fuera de su domicilio particular.

Serán de aplicación a su respecto las normas contenidas en los artículos 2° y 3° del Decreto N° 367/20.

El financiamiento de estas prestaciones será imputado al FONDO FIDUCIARIO DE ENFERMEDADES PROFESIONALES creado mediante el Decreto N° 590/97 de acuerdo a las regulaciones que dicte la SUPERINTENDENCIA DE RIESGOS DEL TRABAJO y deberá garantizarse el mantenimiento de una reserva mínima equivalente al DIEZ POR CIENTO (10 %) de los recursos de este último, con el objeto de asistir el costo de cobertura prestacional de otras posibles enfermedades profesionales, según se determine en el futuro.

ARTÍCULO 7º.- El presente decreto entrará en vigencia a partir del día de su publicación en el BOLETÍN OFICIAL.

ARTÍCULO 8º.- Dese cuenta a la COMISIÓN BICAMERAL PERMANENTE del HONORABLE CONGRESO DE LA NACIÓN.

ARTÍCULO 9º.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

FERNÁNDEZ - Santiago Andrés Cafiero - Eduardo Enrique de Pedro - Agustin Oscar Rossi - Martín Guzmán - Matías Sebastián Kulfas - Alexis Raúl Guerrera - Gabriel Nicolás Katopodis - Luis Eugenio Basterra - Martín Ignacio Soria - Sabina Andrea Frederic - Carla Vizzotti - Daniel Fernando Arroyo - Elizabeth Gómez Alcorta - Nicolás A. Trotta - Tristán Bauer - Roberto Carlos Salvarezza - Claudio Omar Moroni - Juan Cabandie - Matías Lammens - Jorge Horacio Ferraresi - E/E Agustin Oscar Rossi

e. 28/06/2021 N° 44527/21 v. 28/06/2021

Fecha de publicación 28/06/2021

SECTOR PÚBLICO NACIONAL

Decisión Administrativa 641/2021

DECAD-2021-641-APN-JGM - Requisitos mínimos de Seguridad de la Información para Organismos.

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente No EX-2021-00877103-APN-SIP#JGM, la Ley de Ministerios (texto ordenado por Decreto N° 438 del 12 de marzo de 1992 y sus modificatorias), la Ley N° 24.156 y sus modificatorias, los Decretos Nros. 577 del 28 de julio de 2017 y su modificatorio, 50 del 19 de diciembre de 2019 y sus modificatorios, las Decisiones Administrativas Nros. 669 del 20 de diciembre de 2004 y su modificatoria y 1865 del 14 de octubre de 2020, las Resoluciones de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN Nros. 829 del 24 de mayo de 2019 y 1523 del 12 de septiembre de 2019 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1 del 19 de febrero de 2015, y

CONSIDERANDO:

Que por la Decisión Administrativa N° 669/04 se estableció que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias debían dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

Que por el Decreto N° 577/17 modificado por su similar N° 480 del 11 de julio de 2019 se creó el COMITÉ DE CIBERSEGURIDAD en la órbita de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, el cual tiene por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

Que, asimismo, por el citado decreto se encomendó a la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN o a quien esta designara, impulsar los actos administrativos y demás acciones necesarias para la implementación de la Estrategia Nacional de Ciberseguridad que apruebe el COMITÉ DE CIBERSEGURIDAD, así como de los objetivos en ella contenidos.

Que dentro de este marco normativo, por la Resolución N° 829/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN se aprobó la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD y se creó, en el marco del referido COMITÉ DE CIBERSEGURIDAD y en la órbita de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, la Unidad Ejecutiva, cuyas funciones se consignan en el ANEXO II de esa medida.

Que por la Resolución N° 1523/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN se aprobó la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

Que la resolución citada en el considerando anterior define a las Infraestructuras Críticas como aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Que, de igual modo, la mencionada resolución determina como Infraestructuras Críticas de Información a aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

Que se ha producido en los últimos años un incremento sustancial en el uso de las Tecnologías de la Información y las Comunicaciones en el ámbito del Sector Público Nacional, al punto de que se han tornado indispensables para el desenvolvimiento de toda la actividad de las entidades y jurisdicciones que lo componen, tanto en lo que se refiere a la gestión interna como a los servicios que prestan a la sociedad.

Que el intenso uso de las Tecnologías de la Información y las Comunicaciones conlleva asimismo un notable aumento de los riesgos y amenazas a los activos de información y a los sistemas esenciales utilizados para brindar de manera eficiente y constante los múltiples servicios que desde el Sector Público Nacional se prestan.

Que las nuevas formas de ataques informáticos y la actividad maliciosa en general avanzan y se modifican en forma vertiginosa, obligando a mantener actualizadas las herramientas, protocolos y marcos normativos, con el fin de proteger adecuadamente la infraestructura, los activos de información y principalmente los datos personales, que son en definitiva un patrimonio de los ciudadanos en su conjunto.

Que resulta necesario avanzar en el proceso de fortalecimiento de la seguridad de la información que reciben, producen y administran las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, con el fin de dotarlas de las características de confidencialidad, integridad y disponibilidad.

Que por lo expuesto, y atento al incremento, cantidad y variedad de amenazas y vulnerabilidades que rodean a los activos de información, corresponde derogar la Decisión Administrativa N° 669/04 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1/15 -por la que oportunamente se aprobara la “Política de Seguridad de la Información Modelo”-, puesto que las mismas han perdido virtualidad y no reflejan en forma apropiada la situación actual en la materia ni sientan las bases normativas que permitan mantener adecuadamente actualizados los niveles de seguridad de la información que ingresa, y la que generan y producen las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias.

Que si bien la referida Decisión Administrativa N° 669/04 consideraba en el alcance de la norma a las entidades comprendidas en los incisos a) y c) del artículo 8° de la ley citada precedentemente, debido a las características que revisten los requisitos mínimos exigidos se ha considerado más apropiado acotar el alcance de la presente medida a los organismos pertenecientes a la Administración Central y a aquellos descentralizados.

Que, asimismo, la información puede ser objeto de una amplia gama de usos indebidos, debiéndose preservar su confidencialidad, integridad y disponibilidad, con el fin de garantizar la prestación continua e ininterrumpida de los diversos servicios prestados por el Sector Público Nacional.

Que, en este marco, se torna necesario que cada entidad y jurisdicción del Sector Público Nacional comprendida en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias sea capaz de prevenir que sus sistemas de información se vean afectados, implementando, a tal fin, un Plan de Seguridad.

Que a tales fines es indispensable determinar una serie de requisitos mínimos de seguridad para el tratamiento de los datos y los activos de información que gestionan las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, con el fin de adecuarlos a las buenas prácticas y estándares nacionales e internacionales, que contemple tanto la ampliación y profundización en el uso del espacio digital como la emergencia de las nuevas amenazas y riesgos para la confidencialidad, integridad y disponibilidad de la información.

Que, en consecuencia, a los efectos de facilitar la elaboración y ejecución de los Planes de Seguridad mencionados y elevar, a la par, los niveles de seguridad de los sistemas de información de las entidades y jurisdicciones del Sector Público Nacional comprendidos en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, deviene necesario aprobar los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” y establecer todos aquellos recaudos complementarios necesarios.

Que en función de lo expresado es necesario que cada una de las entidades y jurisdicciones del Sector Público Nacional comprendida en el inciso a) del artículo 8° de la Ley N° 24.156 y sus modificatorias asuma la obligación de proteger adecuadamente la información que gestiona, a través de la urgente adopción de medidas preventivas, detectivas y correctivas específicas, destinadas a proteger dicha información y recursos, de conformidad con sus competencias y funciones y en concordancia con los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL”.

Que, consecuentemente, deviene indispensable que cada entidad y jurisdicción alcanzada por la presente decisión administrativa, en el marco del Plan de Seguridad que apruebe y a los fines del cumplimiento de los requisitos de seguridad, apruebe una Política de Seguridad de la Información.

Que la Ley de Ministerios (texto ordenado por Decreto N° 438 del 12 de marzo de 1992 y sus modificatorias) establece entre las atribuciones del Jefe de Gabinete de Ministros la de “Entender en el diseño y ejecución de políticas relativas al empleo público, a la innovación de gestión, a la modernización de la Administración Pública Nacional, al régimen de compras y contrataciones, a las tecnologías de la información, las telecomunicaciones, los servicios de comunicación audiovisual y los servicios postales”.

Que por el Decreto Nº 139 del 4 de marzo de 2021 se incorporó a las funciones que el Decreto N° 50/19 le asignaba a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, el

objetivo de “Entender en la ciberseguridad y protección de infraestructuras críticas de información y comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078”.

Que, asimismo, por el Decreto N° 139/21 antes mencionado se establece además como función de la SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES de la SECRETARÍA DE INNOVACIÓN PÚBLICA, la de “Proponer a la Secretaría estrategias, estándares y regulaciones para la ciberseguridad y protección de infraestructuras críticas de la información y las comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078”.

Que a través de la Decisión Administrativa Nº 1865/20 se aprobó la estructura organizativa del primer y segundo nivel operativo de la JEFATURA DE GABINETE DE MINISTROS, estableciendo como Responsabilidad Primaria de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA la de “Entender en todos los aspectos relativos a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional”.

Que, asimismo, la mencionada decisión administrativa definió, entre las acciones de la citada DIRECCIÓN NACIONAL DE CIBERSEGURIDAD, las de: diseñar políticas de ciberseguridad, en coordinación con los organismos del ESTADO NACIONAL con competencia en la materia; elaborar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, en el ámbito de competencia de la Secretaría; participar en las acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de Ciberseguridad, articulando proyectos con las diferentes áreas del ESTADO NACIONAL involucradas y proponer proyectos de normas relacionados con la ciberseguridad en la REPÚBLICA ARGENTINA, en coordinación con las áreas con competencia en la materia.

Que en este marco resulta pertinente el dictado de un acto administrativo que contribuya a que paulatinamente se incorporen controles que permitan una gestión más responsable, segura y transparente de la información que es tratada por ciertas áreas del Sector Público Nacional.

Que han tomado la intervención de su competencia los servicios jurídicos pertinentes.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 100, inciso 1 de la CONSTITUCIÓN NACIONAL.

Por ello,

EL JEFE DE GABINETE DE MINISTROS

DECIDE:

ARTÍCULO 1°.- Apruébanse los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” que como ANEXO I (IF-2021-50348419-APN-SSTIYC#JGM) forman parte integrante de la presente medida.

ARTÍCULO 2°.- La presente decisión administrativa será de aplicación a las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias y a los proveedores que contraten con esas entidades y jurisdicciones, en todo aquello que se encuentre relacionado con las tareas que realicen y en los términos que establezca cada una de ellas, normativa o contractualmente.

ARTÍCULO 3°.- Las entidades y jurisdicciones del Sector Público Nacional comprendidas en el artículo 2° de esta medida deberán aprobar sus Planes de Seguridad en el plazo máximo de NOVENTA (90) días desde la entrada en vigencia de la presente. Dichos Planes de Seguridad deberán establecer los plazos en que se dará cumplimiento a cada uno de los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” establecidos en el ANEXO I de la presente; plazo que no podrá ser posterior al 31 de diciembre de 2022.

ARTÍCULO 4°.- Los Planes de Seguridad mencionados en el artículo 3° deberán ser remitidos a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA, dependiente de la JEFATURA DE GABINETE DE MINISTROS y/o a la que en el futuro la reemplace, dentro de un plazo máximo de NOVENTA (90) días desde la entrada en vigencia de la presente.

ARTÍCULO 5°.- Las máximas autoridades de las entidades y jurisdicciones comprendidas en el artículo 2° de la presente deberán asignar las funciones relativas a la seguridad de sus sistemas de información al área con competencia en la materia e informar, mediante Comunicación Oficial a través del Sistema de Gestión Documental Electrónica (GDE) a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS el nombre, apellido y datos de contacto del responsable del área designada, dentro del plazo de SESENTA (60) días corridos desde la entrada en vigencia de la presente medida.

ARTÍCULO 6°.- Las entidades y jurisdicciones comprendidas en el artículo 2° de esta medida deberán adoptar las medidas preventivas, detectivas y correctivas destinadas a proteger la información que reciban, generen o gestionen como asimismo sus recursos.

ARTÍCULO 7°.- Las entidades y jurisdicciones establecidas en el artículo 2° de la presente medida deberán reportar a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS los incidentes de seguridad que se produzcan dentro de sus ámbitos, dentro de las CUARENTA Y OCHO (48) horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

ARTÍCULO 8°.- Encomiéndase a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS o a quien esta designe, la revisión y actualización periódica de los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL”, como

asimismo el dictado de las normas complementarias y aclaratorias de la presente medida.

ARTÍCULO 9°.- Deróganse la Decisión Administrativa N° 669 del 20 de diciembre de 2004 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1 del 19 de febrero de 2015.

ARTÍCULO 10.- Invítase a las entidades y jurisdicciones enumeradas en los incisos b), c) y d) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, a los Gobiernos Provinciales, de la Ciudad Autónoma de Buenos Aires y Municipales, y a los Poderes Legislativo y Judicial de la Nación a adherir a la presente.

ARTÍCULO 11.- La DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS verificará el cumplimiento de las disposiciones de la presente medida, sin perjuicio de las competencias asignadas a la SINDICATURA GENERAL DE LA NACIÓN.

ARTÍCULO 12.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Santiago Andrés Cafiero - Eduardo Enrique de Pedro

NOTA: El/los Anexo/s que integra/n este(a) Decisión Administrativa se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 28/06/2021 N° 44521/21 v. 28/06/2021

Fecha de publicación 28/06/2021

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Anexo

Número: IF-2021-50348419-APN-SSTIYC#JGM

CIUDAD DE BUENOS AIRES
Viernes 4 de Junio de 2021

Referencia: ANEXO I - REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SPN

ANEXO I

REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN [1]

PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL

I. INTRODUCCIÓN

Los organismos del Sector Público Nacional comprendidos en el artículo 8º de la Ley Nº 24.156 y sus modificatorias son de los principales receptores y productores de información de nuestro país. Esa información pertenece mayormente a sus habitantes y a las diversas entidades públicas y privadas que desarrollan sus actividades en su territorio. Todos ellos confían sus datos a los organismos que lo componen para distintos fines.

La información puede ser hoy en día objeto de una amplia gama de peligros, amenazas y usos indebidos e ilícitos, debiéndose, por lo tanto, extremar las medidas tendientes a la preservación de su confidencialidad, integridad y disponibilidad. Con esto se busca proteger los derechos y libertades individuales de las personas al tiempo de contribuir a la efectiva prestación continua e ininterrumpida de los diversos servicios prestados por las diferentes entidades y jurisdicciones y, al mismo tiempo, propender a su correcta y mejor gestión interna.

En un contexto de transversalidad en el uso de las tecnologías para la vida social, económica, política y cultural de las personas, la seguridad de la información cumple un rol fundamental. Por consiguiente, los agentes públicos, cualquiera sea el nivel jerárquico y la modalidad de contratación, tienen la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos.

Los responsables de los activos de la información deben atender y diligenciar los recursos necesarios para asegurar el cumplimiento de los objetivos de la presente en el ámbito de su jurisdicción. En tal sentido, los datos gestionados en los organismos deben ser protegidos tanto dentro como fuera del ámbito institucional, con independencia del formato y del soporte en el que estén contenidos y si los mismos están siendo objeto de tratamiento electrónico, se encuentran almacenados o están siendo transmitidos.

Los organismos determinarán sus políticas, normas específicas, procedimientos y guías que, sobre la base de los siguientes requisitos mínimos, sean aplicables a los procesos específicos que desarrollen. Este conjunto de normas debe surgir a partir de un análisis de los riesgos para los procesos que lleven adelante.

Se entenderán como principios de seguridad de la información a la preservación de confidencialidad, integridad y disponibilidad de la información y de los activos de información del Sector Público Nacional.

II. OBJETIVOS

Objetivo general

Establecer los lineamientos generales y mínimos para los organismos del Sector Público Nacional comprendidos en el inciso a) del artículo 8º de la Ley Nº 24.156, con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

Objetivos específicos

- Proteger los derechos de los titulares de datos personales o propietarios de información que es tratada por el Sector Público Nacional.
- Proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional.
- Promover una política pública que enmarque una conducta responsable en materia de seguridad de la información de los organismos que conforman el Sector Público Nacional, sus agentes y funcionarios.
- Evidenciar el compromiso e interés de quienes componen el Sector Público Nacional en pos del desarrollo de una cultura de ciberseguridad.

III. ALCANCE

Las directrices que surgen de los presentes requisitos mínimos de seguridad serán de aplicación obligatoria para todos los agentes y funcionarios que se desempeñan en los organismos que componen el Sector Público Nacional según el inciso a) del artículo 8º de la Ley Nº 24.156 y sus modificatorias, en la medida que les corresponda según su función. Las autoridades máximas de los organismos públicos serán las responsables de proveer los medios necesarios para su efectivo cumplimiento y de promover su utilización.

En el caso de los entes reguladores que estén comprendidos dentro del artículo 8º de la Ley Nº 24.156 y sus modificatorias, se recomienda el análisis de una eventual incorporación de los principios de la Seguridad de la

Información. Asimismo, se sugiere la evaluación de la oportunidad y pertinencia de establecer requisitos mínimos de seguridad de la información que más adelante se detallan en la sección V. Directrices, para el sector regulado.

El cumplimiento de los presentes requisitos mínimos de seguridad será también exigible a los terceros que contraten con el Sector Público Nacional, en las secciones que sean aplicables a las tareas que realizan y en los términos que establezca cada organismo en sus disposiciones normativas y contractuales.

IV. REVISIÓN Y ACTUALIZACIÓN

Los requisitos mínimos de Seguridad serán revisados por la Dirección Nacional de Ciberseguridad de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, o el área que la reemplace en el futuro, cuando lo estime conveniente, con una periodicidad no superior a DOCE (12) meses, a partir de su publicación o última actualización. Serán publicados también en el sitio de Internet que, a tal fin, establezca la Dirección Nacional antes citada.

V. DIRECTRICES

1. Política de Seguridad de la Información del organismo

Los organismos deben desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlos. Los términos de dicha política deben ser consistentes con las directrices del presente documento.

Dicha política debe ser:

- aprobada por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.
- notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.
- cumplida por todos los agentes y funcionarios del organismo.
- revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.
- utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.
- informada a la Dirección Nacional de Ciberseguridad una vez aprobada.

2. Aspectos Organizativos de la Seguridad

Se debe desarrollar e implementar un marco organizativo que habilite una efectiva gestión y operación de la seguridad de la información en el organismo.

Esto implica que se debe:

- asignar a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información, incluyendo el cumplimiento de las directrices del presente documento. Se

deberá informar a la Dirección Nacional de Ciberseguridad el nombre y datos de contacto del responsable del área a la que se le han asignado las funciones y mantener dichos datos actualizados.

- segregar las funciones y áreas de responsabilidad en conflicto para incrementar los niveles de seguridad de la información. En la medida de lo posible, se recomienda que las funciones de seguridad de la información no dependan del área de Sistemas o Tecnología de la Información.
- impulsar desde el mayor nivel jerárquico las iniciativas que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona.
- abordar los aspectos referidos a la seguridad de la información en el diseño y la gestión de todos los proyectos que lleve adelante el organismo, dejando evidencia de tal intervención.
- establecer como falta, sobre la base del régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias, el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, por parte de los agentes y funcionarios, incluyendo una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.
- incluir en los contratos, Términos de Referencia o en el instrumento mediante el cual se materialice la contratación del personal que se emplee bajo las modalidades que correspondan, cláusulas que contemplen el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, incluyendo una graduación en las responsabilidades y sanciones que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.
- establecer mecanismos adecuados de seguridad para el trabajo remoto y para el uso de dispositivos móviles, sean estos provistos por el organismo o propiedad de agentes y funcionarios, según la criticidad de la información involucrada y del nivel jerárquico del funcionario.

3. Seguridad Informática de los Recursos Humanos

Los organismos deben adoptar una perspectiva sistémica para proteger sus activos de información, dentro de la cual el personal debe ser considerado un recurso central. Asimismo, deben establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad. Los agentes y funcionarios deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos.

Para ello será necesario:

- realizar e implementar planes de concientización en el uso seguro y responsable de los activos de información, que incluyan capacitaciones periódicas destinadas a todos los agentes y funcionarios del organismo, diseñándolos para cada tipo de público y con distintas temáticas.
- promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.
- establecer la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información para todos los empleados del organismo, cualquiera sea su modalidad de contratación, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.
- establecer claramente los requerimientos de seguridad de la información, que incluya niveles de acceso a la

información para cada perfil de trabajo.
- incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.
- requerir a los agentes y funcionarios, cuando el organismo lo considere necesario, de acuerdo a sus competencias, la firma de un acuerdo de confidencialidad.
- incorporar dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo.

4. Gestión de Activos

Los activos de información del organismo deben ser gestionados y protegidos en forma efectiva. En el mismo sentido, deben ser clasificados según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, teniendo en cuenta sus funciones, la normativa que les sea aplicable y cualquier otro activo que pudieran contener de otros organismos públicos o entidades privadas, lo que permitirá adoptar las medidas de protección adecuadas.

Para ello se requiere:

- clasificar los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.
- llevar un inventario actualizado en el que se detallen los datos necesarios para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.
- exigir a todos los agentes y empleados la devolución de los activos de información en su poder al finalizar la relación laboral o cuando un cambio en las funciones lo requiera.
- efectuar una destrucción segura de cualquier medio que pueda contener información o datos personales, en función de su nivel de criticidad, sobre la base de un procedimiento documentado, una vez que se haya catalogado como defectuoso o rezago.

5. Autenticación, Autorización y Control de Accesos

El acceso a los activos de información del organismo debe realizarse a partir de procesos y mecanismos de seguridad definidos e implementados según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. Los privilegios de acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones.

En consiguiente se debe:

- utilizar en todos los casos el principio de “necesidad de saber”, es decir que solo se otorguen privilegios de acceso en la medida en que sean requeridos para las actividades y tareas que cada empleado o funcionario debe llevar adelante.
- hacer una adecuada y oportuna gestión de las altas y bajas de cuentas de usuario y privilegios, coordinando con las áreas de Recursos Humanos y aquellas en las que el empleado se desempeña toda novedad que pudiera impactar en ellos.
- realizar un seguimiento detallado sobre las cuentas con privilegios especiales.
- revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.
- requerir a los agentes, funcionarios y demás usuarios un uso responsable de sus dispositivos y datos de autenticación, dejando sentado que se encuentra estrictamente prohibido compartirlos y que deben ser mantenidos seguros en forma permanente.

- restringir y controlar la asignación y uso de derechos de accesos privilegiados.
- limitar y monitorear el acceso al código fuente de los programas.

6. Uso de herramientas criptográficas

La confidencialidad, integridad, autenticidad y/o no repudio de la información del organismo debe ser protegida mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.

En este marco se debe:

- requerir el cifrado de cualquier dispositivo del organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.
- proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.
- utilizar certificados digitales en todos los sitios de Internet del organismo.

7. Seguridad física y ambiental

Los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.

Esto implica:

- la identificación y protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales.
- la incorporación de controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.
- el registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.
- la adopción de medidas de seguridad para que el equipamiento sea ingresado o retirado del organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.
- el cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.
- la adopción de medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del organismo y la interrupción de sus operaciones.
- la protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.
- el mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continuas.
- la adopción de medidas de seguridad para los activos informáticos que deben llevarse fuera del organismo, considerando los distintos riesgos de trabajar fuera de sus dependencias, en lo que hace al resguardo de la información y a la seguridad física de los dispositivos.

8. Seguridad operativa

Las operaciones del organismo deben desarrollarse en forma segura, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para ello se debe:

- establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.
- revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.
- minimizar los riesgos de acceso o de cambios no autorizados en entornos productivos, separando los entornos de desarrollo, prueba y producción, en los casos que corresponda.
- implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.
- proteger las instalaciones contra infecciones de código malicioso.
- realizar copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.
- llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes.
- mantener un control estricto sobre el software y su integridad, en entornos productivos.
- identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación.
- gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.
- registrar y revisar periódicamente las actividades de los administradores y operadores.

9. Seguridad en las comunicaciones

La información de las redes del organismo debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.

Se debe:

- Segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.
- proteger adecuadamente la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.
- exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.
- incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.

10. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites

a través de Internet.

Para ello se debe:

- especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.
- utilizar una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.
- controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción e incorporando efectivos controles cruzados o por oposición.
- proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.
- utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.
- evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.
- proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.
- controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el cocontratante en aquellas contrataciones de bienes y servicios efectuadas por el organismo.

11. Relación con proveedores

La contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio debe incluir en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del cocontratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

Esto comprende:

- la consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.
- el establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al organismo.
- la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.
- la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.
- la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.

12. Gestión de incidentes de seguridad

El organismo debe adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

Para ello debe:

- identificar las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.
- contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.
- adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.
- instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.
- notificar a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.
- recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.
- en el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.

13. Aspectos de seguridad para la continuidad de la gestión

Los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales deben contemplar todos los aspectos de seguridad de la información involucrada.

Para ello se debe:

- identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.
- establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.
- verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.
- implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

14. Cumplimiento

En todos los casos el organismo debe cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.

Esto implica:

- la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.

- el cumplimiento de la Ley Nº 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.
- la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.
- la supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.
- considerar la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.

VI. Glosario

Los términos utilizados en este documento se encuentran incluidos en el Glosario aprobado por la Resolución N° 1523/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN y en la Ley Nº 25.326 de Protección de los Datos Personales.

---

[1] Para la elaboración del presente documento se han tomado como referencia estándares nacionales e internacionales reconocidos, tales como las Normas IRAM-ISO/IEC 27001, 27002 y 20000-1.

Digitally signed by Gestion Documental Electronica
Date: 2021.06.04 18:04:28 -03:00

Martín OLMOS
Subsecretario
Subsecretaría de Tecnologías de la Información y las Comunicaciones
Jefatura de Gabinete de Ministros

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO

Resolución 62/2021

RESOL-2021-62-APN-SGYEP#JGM

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente N° EX-2021-56258684- -APN-SGYEP#JGM, del Registro de la JEFATURA DE GABINETE DE MINISTROS, las Leyes Nº 27.491, N° 27.541 y sus modificatorios y N° 27.573, los Decretos N° 260 del 12 de marzo de 2020 y sus modificatorios y N° 287 del 30 de abril de 2021 y sus modificatorios, la Decisión Administrativa Nº 390 del 16 de marzo de 2020 y su modificatoria, las Resoluciones del MINISTERIO DE SALUD N° 627 del 19 de marzo del 2020 y su modificatoria y N° 2883 del 29 de diciembre de 2020, la Resolución Conjunta del MINISTERIO DE SALUD y el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL Nº 4 del 8 de abril de 2021, y

CONSIDERANDO:

Que mediante la Ley de Solidaridad Social y Reactivación Productiva N° 27.541 se declaró la emergencia pública en materia económica, financiera, fiscal, administrativa, previsional, tarifaria, energética, sanitaria y social.

Que, posteriormente, a través del Decreto N° 260 del 12 de marzo de 2020 y sus modificatorios se amplió la emergencia pública en materia sanitaria con motivo de la pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el nuevo coronavirus COVID-19 por el plazo de UN (1) año desde su entrada en vigencia, el cual fue prorrogado por el Decreto Nº 167 del 11 de marzo de 2021 hasta el día 31 de diciembre de 2021, y se facultó al MINISTERIO DE SALUD DE LA NACIÓN a adoptar las medidas que resulten oportunas y necesarias para la prevención de la propagación del SARS-CoV-2, con el objeto de minimizar sus efectos e impacto sanitario.

Que, ante la actual situación epidemiológica y el acelerado aumento de casos, mediante el Decreto Nº 287 del 30 de abril de 2021 y sus modificatorios se implementó la clasificación de las situaciones de riesgo epidemiológico, asociadas con medidas temporarias, intensivas, focalizadas geográficamente y orientadas a las actividades y horarios que conllevan mayores riesgos, que incluyeron a las organizaciones y las y los trabajadores del Sector Público.

Que la norma mencionada en el párrafo anterior, se encuentra vigente y prorrogada por el Decreto N° 381 del 11 de junio de 2021.

Que, sin perjuicio de lo anterior, cabe destacar que por Ley N° 27.491 se declaró la vacunación de interés nacional, entendiéndosela como una estrategia de salud pública preventiva y altamente efectiva, y considerándosela como un bien social, sujeto a principios de gratuidad, interés colectivo, disponibilidad y amplia participación.

Que contar con una vacuna segura y eficaz para prevenir el COVID-19 es determinante para controlar el avance de la enfermedad, ya sea disminuyendo la morbimortalidad o la transmisión del virus, y permite mejorar el cuidado de la vida y la salud de los y las habitantes del país, así como restablecer paulatinamente las actividades económicas y sociales.

Que por Resolución del MINISTERIO DE SALUD N° 2883 del 29 de diciembre de 2020 se aprobó el “Plan Estratégico para la Vacunación contra la COVID-19 en la República Argentina”, el cual establece una estrategia de vacunación voluntaria, escalonada y en etapas no excluyentes, procurando ampliar progresivamente la población objetivo y permitiendo inmunizar de forma gradual a mayor cantidad de personas.

Que el Estado Nacional suscribió diversos acuerdos tendientes a la adquisición de vacunas en tiempo oportuno, lo cual permitió iniciar la vacunación en las VEINTICUATRO (24) jurisdicciones del país de manera simultánea en el mes de diciembre pasado.

Que en la “II Reunión extraordinaria de la Comisión Nacional de Inmunización”, desarrollada el 1° de marzo de 2021, se instó a la elaboración de recomendaciones sobre el impacto de la vacunación en las licencias laborales y el potencial retorno a la actividad laboral de las personas vacunadas.

Que, de acuerdo con lo expresado en los fundamentos de la Resolución Conjunta del MINISTERIO DE SALUD y el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL Nº 4 del 8 de abril de 2021, según los resultados disponibles al momento las vacunas utilizadas en Argentina demostraron una adecuada eficacia para la prevención de las formas graves y de la muerte por la enfermedad, lo cual disminuye el riesgo y posibilita el retorno de las personas vacunadas a sus lugares de trabajo.

Que, con fecha 26 de marzo de 2021, el MINISTERIO DE SALUD comunicó, en virtud de lo acordado con todas las jurisdicciones en el marco del Consejo Federal de Salud (COFESA), nuevas recomendaciones relacionadas con la priorización de la primera dosis de las vacunas contra COVID-19 en la población objetivo, difiriendo la segunda dosis de cualquiera de las vacunas actualmente disponibles en nuestro país a un intervalo mínimo de DOCE (12) semanas desde la primera dosis.

Que dicha recomendación, que hace referencia a la extensión del intervalo mínimo sugerido entre ambas dosis y no a la suspensión de la segunda dosis, tiene como fin proteger lo antes posible a la mayor cantidad de personas con alguna condición de riesgo y reducir el impacto de las muertes por esta enfermedad.

Que todo lo anterior permite el establecimiento de pautas para el retorno a la actividad laboral presencial en contexto de pandemia de las personas trabajadoras vacunadas, con la debida observancia de las recomendaciones sanitarias en materia de prevención y control de la salud pública, sin poner en peligro los esquemas implementados para evitar la propagación del nuevo coronavirus SARS-CoV-2, virus responsable del COVID-19.

Que mediante la citada Resolución Conjunta Nº 4/21, se dispuso para el Sector Privado que los empleadores y las empleadoras podrán convocar al retorno a la actividad laboral presencial a las personas trabajadoras, incluidas las dispensadas por encontrarse comprendidas en los incisos a), b) y c) del artículo 1° de la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 207 del 16 de marzo de 2020 y sus modificatorias, que hubieren recibido al menos la primera dosis de cualquiera de las vacunas destinadas a generar inmunidad adquirida contra el COVID-19 autorizadas para su uso en la República Argentina, independientemente de la edad y la condición de riesgo, transcurridos CATORCE (14) días desde la inoculación.

Que la mencionada Resolución Conjunta fijó el criterio de adquisición de inmunidad, a los fines de la convocatoria de asistencia a los lugares de trabajo.

Que actualmente, la reducción de casos de COVID-19 positivos ha reducido la emergencia del sistema sanitario, por lo que resulta oportuno y conveniente la aplicación del criterio de convocatoria a los lugares de trabajo en el Sector Público Nacional.

Que la DIRECCIÓN NACIONAL de la OFICINA NACIONAL DE EMPLEO PÚBLICO de la SUBSECRETARÍA DE EMPLEO PÚBLICO de la SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS, se ha expedido en el ámbito de su competencia

Que mediante IF-2021-56983345-APN-DGAJ#JGM la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARÍA LEGAL de la SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, ha tomado la intervención de su competencia

Que la presente medida se dicta en uso de las facultades previstas por el artículo 2° del Anexo I del Decreto N° 1421 del 8 de agosto de 2002 y sus modificatorios, y por el Decreto N° 50 del 19 de diciembre de 2019 y sus modificatorios.

Por ello,

LA SECRETARIA DE GESTIÓN Y EMPLEO PÚBLICO DE LA JEFATURA DE GABINETE DE MINISTROS

RESUELVE:

ARTÍCULO 1º.- Establécese que las y los titulares de cada jurisdicción, organismo o entidad comprendido en el artículo 8° de la Ley N° 24.156 y sus modificatorios, podrán convocar al retorno a la actividad laboral presencial a las y los trabajadores que hubieren recibido al menos la primera dosis de cualquiera de las vacunas destinadas a generar inmunidad adquirida contra el COVID-19 autorizadas para su uso en la REPÚBLICA ARGENTINA, independientemente de la edad y la condición de riesgo, transcurridos CATORCE (14) días de la inoculación.

ARTÍCULO 2°.- Las personas trabajadoras de la salud con alto riesgo de exposición que se encuentren comprendidas en los incisos 2) y 3) del artículo 1° de la Decisión Administrativa Nº 390 del 16 de marzo de 2020 y su modificatoria, podrán ser convocadas una vez transcurridos CATORCE (14) días de haber completado el esquema de vacunación en su totalidad, independientemente de la edad y la condición de riesgo, sin perjuicio de lo

establecido en el artículo 5° de la presente.

ARTÍCULO 3º.- Las personas convocadas deberán presentar constancia fehaciente de vacunación correspondiente o manifestar, con carácter de declaración jurada, los motivos por los cuales no pudieron acceder a la vacunación.

ARTÍCULO 4º.- Las personas comprendidas en el ámbito alcanzado por la medida dispuesta en los artículos 1º y 2º de la presente resolución que tengan la posibilidad de acceder a la vacunación y opten por no vacunarse, deberán actuar de buena fe y llevar a cabo todo lo que esté a su alcance para evitar los perjuicios que su decisión pudiere ocasionar al normal desempeño de las organizaciones en las cuales prestan servicios.

ARTÍCULO 5°.- Exceptúase a las personas incluidas en el artículo 3°, incisos V y VI de la Resolución del MINISTERIO DE SALUD N° 627 del 19 de marzo de 2020 y su modificatoria, de lo previsto por los artículos 1° y 2º de la presente resolución.

ARTÍCULO 6°.- La presente medida comenzará a regir a partir del día de su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

ARTÍCULO 7°.- Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Ana Gabriela Castellani

e. 28/06/2021 N° 44514/21 v. 28/06/2021

Fecha de publicación 28/06/2021

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE INNOVACIÓN PÚBLICA

Resolución 65/2021

RESOL-2021-65-APN-SIP#JGM

Ciudad de Buenos Aires, 24/06/2021

VISTO el Expediente Electrónico N.° EX-2021-54431188-APN-SSGAIP#JGM, la Ley N.° 23.396, el Decreto N.° 945 de fecha 17 de noviembre de 2017, el Decreto N.° 50 de fecha 19 de diciembre de 2019 y sus modificatorios, el Decreto N.° 86 de fecha 27 de diciembre de 2019, el Documento del Proyecto PNUD ARG/20/008, y

CONSIDERANDO:

Que por el Expediente citado en el Visto, tramita un proyecto de Resolución tendiente a crear el Programa “Becas País Digital”.

Que mediante la Ley N.º 23.396, se aprobó el Acuerdo entre la República Argentina y el Programa de las Naciones Unidas para el Desarrollo (PNUD) firmado en Buenos Aires el 26 de febrero de 1985, en el cual se enuncian las condiciones básicas en las cuales el PNUD y sus Organismos de Ejecución prestarán asistencia al gobierno para llevar a cabo sus proyectos de desarrollo.

Que en el marco de la Ley precitada, se suscribió el Documento de Proyecto (PRODOC) del Proyecto PNUD ARG/20/008, denominado “Promoción de la inclusión digital y la igualdad a través de la Innovación Pública Federal”, en cuya Actividad N.° 3, “Apoyar la innovación de la gestión y administración pública eficaz para un gobierno abierto y digital inclusivo”, se estableció como objetivo la contratación de servicios de Universidades dedicadas a la formación de personas en habilidades digitales para llevar a cabo actividades de capacitación, dirigidas a personas mayores de 18 años con estudios de nivel secundario finalizados y que no se encuentren en el momento siendo beneficiarios de otra beca educativa otorgada por el Estado.

Que a través del Decreto N° 50/19, se aprobó el Organigrama de Aplicación de la Administración Nacional centralizada hasta nivel de Subsecretaría, creándose, entre otras, la SECRETARÍA DE INNOVACIÓN PÚBLICA dependiente de la JEFATURA DE GABINETE DE MINISTROS, entre cuyos objetivos se encuentra el de “Entender en la promoción del acceso universal a las nuevas tecnologías como herramientas de información y conocimiento (…)”.

Que con fecha 17 de noviembre de 2017, mediante el Decreto N° 945, se estableció que las “Jurisdicciones y Entidades de la Administración Pública Nacional comprendidas en el artículo 8° inciso a) de la Ley Nº 24.156 que ejecuten programas y proyectos con financiamiento externo multilateral, bilateral o regional y/o proyectos de participación público-privada a través de las unidades ejecutoras creadas a tal efecto, centralizarán la gestión y ejecución operativa, administrativa, presupuestaria y financiera-contable, comprendiendo las cuestiones fiduciarias y legales, sobre cumplimiento de las cuestiones ambientales y sociales, los procedimientos de contrataciones, como así también, la planificación, programación, monitoreo y auditoría de dichos programas y proyectos, a través de sus respectivas Subsecretarías de Coordinación Administrativa o áreas equivalentes, según corresponda.”.

Que, asimismo, mediante el artículo 2° de dicho Decreto, se estipuló que “Las funciones de coordinación y ejecución técnica de los programas y proyectos con financiamiento externo multilateral, bilateral o regional y/o proyectos de participación público-privada, actualmente desarrolladas por las unidades ejecutoras técnicas o por las áreas técnicas de unidades ejecutoras de programas, serán llevadas a cabo por las Secretarías y Subsecretarías o áreas equivalentes de carácter sustantivo de las Jurisdicciones y Entidades comprendidas por el artículo 8° inciso a) de la Ley Nº 24.156 con responsabilidad primaria en la materia de que se trate.”.

Que, en sentido concordante, por el ya citado Decreto N° 50/19, se estableció, entre los objetivos a cargo de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA, dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA, el de “Entender en la ejecución operativa y en los procesos de gestión administrativa, presupuestaria y financiera-contable de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo, como así también en los proyectos de participación público-privada, en coordinación con las áreas pertinentes de la SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA.”.

Que, por su parte, entre los objetivos a cargo de la SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, establecidos en la precitada norma, se encuentra el de “Promover la creación de una red de innovación pública y gobierno abierto a nivel nacional generando espacios de trabajo colaborativo, intercambio y capacitación con el Sector Público Nacional, Provincial, de la Ciudad Autónoma de Buenos Aires y Municipal, el sector privado, académico y organizaciones de la sociedad civil” y el de “Asistir a la Secretaría en la promoción de políticas, programas y acuerdos de innovación pública en el territorio nacional, en particular en las Jurisdicciones provinciales, municipales y en la CIUDAD AUTÓNOMA DE BUENOS AIRES.”.

Que la creación del Programa “Becas País Digital” se funda en la necesidad de fomentar la inclusión digital y la participación de mujeres y diversidades en la industria de las Tecnologías de la Información y las Comunicaciones (TIC), constituyendo, asimismo, una acción de capacitación que promueva una formación integral que incluya conocimientos de programación, marketing digital y ciencia de datos, todo lo cual coadyuvará a dar respuesta a la demanda laboral de personas calificadas en habilidades digitales.

Que, atento lo hasta aquí expuesto, a fin de dar cumplimiento al objetivo señalado en el párrafo cuarto de la presente, resulta necesario crear el Programa “Becas País Digital”.

Que, asimismo, atento razones de eficiencia, resulta conveniente delegar su planificación, programación, gestión y ejecución en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la

SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, ambas dependientes de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que, al mismo tenor, resulta pertinente facultarlos para dictar las medidas complementarias a la presente y para suscribir convenios específicos y/o acuerdos con cámaras empresariales o entidades pertinentes a fin de cumplimentar los objetivos del Programa.

Que el gasto que demande la presente se atenderá con cargo a las partidas específicas del PROYECTO PNUD ARG/20/008 y del SAF 366 Jurisdicción 25 de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que la DIRECCIÓN DE ASUNTOS LEGALES DE INNOVACIÓN PÚBLICA, dependiente de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA de la SECRETARÍA DE INNOVACIÓN PÚBLICA, ha tomado la intervención de su competencia.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el Decreto N° 50/19 y por el Decreto N° 86/19.

Por ello,

LA SECRETARIA DE INNOVACIÓN PÚBLICA

RESUELVE:

ARTÍCULO 1°.- Créase el Programa “BECAS PAÍS DIGITAL” con el objeto de fomentar la inclusión digital y la participación de mujeres y diversidades en la industria de las Tecnologías de la Información y las Comunicaciones (TIC) y de capacitar en programación, marketing digital y ciencia de datos, a fin de responder a la demanda laboral de personas calificadas en habilidades digitales.

ARTÍCULO 2°.- Delégase la planificación, programación, gestión y ejecución del Programa creado en el artículo primero en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, ambas dependientes de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, quedando facultadas – en forma conjunta – para dictar las medidas complementarias a la presente y para suscribir convenios específicos y/o acuerdos específicos con cámaras empresariales o entidades pertinentes a fin de cumplimentar los objetivos de aquel.

ARTÍCULO 3°.- Delégase en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la SUBSECRETARIA DE GOBIERNO ABIERTO Y PAÍS DIGITAL la facultad, en forma conjunta, de aprobar las definiciones y el reglamento de bases y condiciones para la convocatoria “BECAS PAÍS DIGITAL”.

ARTÍCULO 4°.- El gasto que demande la presente medida sera atendido con cargo a las partidas específicas del PROYECTO PNUD ARG/20/008 y del SAF 366 Jurisdicción 25 de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

ARTÍCULO 5°.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Micaela Sánchez Malcolm

e. 28/06/2021 N° 44104/21 v. 28/06/2021

Fecha de publicación 28/06/2021

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Informe

Número: IF-2021-53649652-APN-SSCPU#JGM

CIUDAD DE BUENOS AIRES
Martes 15 de Junio de 2021

Referencia: PROGRAMA SUMAR CAPACITACIÓN

Anexo I

PROGRAMA "SUMAR CAPACITACIÓN"

I. Fundamentación

A partir de las Misiones y Funciones de la SECRETARIA DE MEDIOS Y COMUNICACIÓN PÚBLICA vinculadas a fortalecer la libertad de expresión e impulsar la pluralidad cultural e informativa, se busca establecer el presente programa que consiste en la puesta en funcionamiento de un dispositivo de capacitación en pos de generar una estrategia de formación continua destinada a los actores de comunicación participantes de Medios de Gestión Social de todo el país.

En ese marco se pretende fomentar el empoderamiento de los medios de gestión social mediante el aporte de nuevos conocimientos y el perfeccionamiento de sus capacidades actuales tanto para la generación de contenidos de mayor calidad como así también para su vinculación con el público en general.

Así es posible desarrollar distintas iniciativas de formación integral en materia de comunicación destinada a impulsar herramientas que permitan involucrarse activamente a todos aquellos actores que desean participar como productores de la circulación informativa y de sentido en la sociedad.

En ese sentido, este Programa promueve la articulación e implementación de cursos de capacitación en conjunto

con asociaciones civiles sin fines de lucro, organizaciones sindicales, universidades nacionales, instituciones educativas terciarias y gobiernos locales entre otros actores; entendiendo que la comunicación actual demanda acciones permanentes del Estado orientadas a la profesionalización y reflexión crítica sobre el funcionamiento de los medios de comunicación.

II. Objetivos:

Objetivos generales:

. Promover articulaciones del Estado con los medios de gestión social de todas las regiones del país.

. Promover la formación como proceso permanente y necesario con miras al fortalecimiento de la pluralidad informativa

. Promover el fortalecimiento vincular con las organizaciones asociadas a la comunicación.

. Promover miradas y análisis críticos vinculadas al desarrollo de la comunicación

. Contribuir a la apropiación de herramientas conceptuales y políticas como parte del proceso de reconocimiento de la comunicación comunitaria.

. Garantizar el cuestionamiento a los modelos imperantes que reproducen los medios de comunicación masivos.

III. Finalidad

Apuntamos que al finalizar el proceso de formación lxs participantes se encuentren fortalecidxs para el ejercicio cotidiano de su desarrollo en el ámbito de la comunicación.

IV. Destinatarixs

Todas aquellas personas vinculadas de manera directa con los medios de gestión social, en cualquiera de sus formatos.

Asimismo, se invita a asociaciones civiles sin fines de lucro, organizaciones sindicales, universidades nacionales, instituciones educativas terciarias y gobiernos locales para la proyección de las distintas actividades curriculares.

V. Articulaciones institucionales

Consideramos indispensable abonar al intercambio con aquellas organizaciones con conocimiento en comunicación comunitaria, trayectoria en trabajo en ese campo, y acompañamientos de los medios en los diversos territorios.

El Programa conformará un equipo para dar respuesta a las necesidades del territorio que puedan ser abordadas desde la formación, garantizando la sinergia entre la Subsecretaría de contenidos públicos y las actorxs de la comunicación comunitaria.

A su vez, será responsabilidad de este equipo garantizar la evaluación continua y de proceso en la preparación y ejecución de los proyectos, garantizando un monitoreo de resultados que permitan asegurar el cumplimiento de los objetivos y, al mismo tiempo, mejorar el accionar del Programa.

VI. Modalidad de Trabajo

El programa consiste en la generación y puesta en funcionamiento de cursos de capacitación por parte de las asociaciones civiles con las cuales se suscribirán convenios específicos a tal efecto.

Los cursos contemplan una duración total de cuarenta y ocho (48) horas a desarrollarse en un plazo de dos meses. El tutor a cargo de los mismos deberá brindar seis (6) horas semanales, divididas en dos (2) horas de presentación y explicación de los contenidos de la clase de manera virtual; dos (2) horas de tareas de seguimiento de las actividades en la plataforma; dos (2) horas de trabajo en conjunto de los contenidos trabajados en la semana y el debate correspondiente a partir de las lecturas.

Es tarea de la parte conveniada determinar en primer término un referente del proyecto; presentar los contenidos de acuerdo a los lineamientos y objetivos del Programa; dictar la totalidad de horas de clases proyectadas; deberá contar con un equipo que garantice la articulación de la propuesta pedagógica, el seguimiento administrativo y la rendición de cuentas.

La Subsecretaría de contenidos públicos tiene a su cargo la coordinación general del Programa, su implementación y monitoreo.

Para garantizar los objetivos propuestos se priorizará y trabajará para la federalización del Programa, tanto en lo

comunicacional, en la selección de proyectos, como así también en su acompañamiento y adecuación que aseguren la posibilidad de acceder al mismo teniendo en cuenta las particularidades de lxs destinatarixs.

VII. Ejes generales para los cursos a desarrollarse en el periodo 2021/22

- Radio para adultos mayores.
- Radio I
- Radio II
- Realización de podcast
- Radioteatro
- Taller de locución
- Edición de sonido
- Nuevas Tecnologías en radio
- Producción periodística y Creatividad en radio
- Producción informativa
- Edición Artística
- Operación Técnica en Radio
- Marketing Digital
- Producción de videos en dispositivos móviles
- Taller de periodismo multimedia
- Cobertura inclusiva: perspectiva de género en las salas de redacción | discapacidad
- Community Manager
- Taller de fotoperiodismo móvil
- Utilización de herramientas Google | Analytics Google ads

- Comunicación efectiva
- Curso de oratoria
- Cybersegurdiad
- Aspectos legales para la creación de un medio de comunicación I
- Aspectos legales para la creación de un medio de comunicación II
- Registro de marca
- Plataformas Digitales
- Geomarketing
- Diseño web
- Introducción a software libre
- Social Media manager | Redes sociales como medio de comunicación
- Comercialización

VIII. Financiamiento

La Secretaría de medios y comunicación pública otorgará a la entidad conveniada la suma de pesos ciento cincuenta y ocho mil cuatrocientos ($158.400) por cada curso dictado conforme los lineamientos establecidos en el programa. La suma establecida surge de los siguientes parámetros

- Pesos setenta y dos mil ($72.000). - equivalente al sueldo del tutor, a un valor de $1.500.- la hora, conforme a seis (6) horas semanales por dos (2) meses;
- Pesos setenta y dos mil ($72.000) con motivo de la producción del curso;
- 10% sobre el total (Curso + sueldo) para tareas administrativas.

Para el año 2021 se prevé la generación de un total de veinticinco cursos de SUMAR CAPACITACIÓN por lo cual se requerirá a tal fin de un presupuesto de PESOS TRES MILLONES NOVECIENTOS SESENTA MIL

($3.960.000,00).

IX. Requisitos para la presentación de propuestas

La Subsecretaría de contenidos públicos tendrá a su cargo el establecimiento de los requisitos que deberán ser cumplidos por las entidades y organizaciones sociales que soliciten la producción y dictado de cursos en el marco del presente programa.

X. Rendición de cuentas e incumplimientos.

La Subsecretaría de contenidos públicos será la encargada de la implementación y control del mecanismo de rendición respecto al curso o cursos conveniados. Asimismo en caso de verificarse un incumplimiento total o parcial del proyecto conveniado en ningún caso se concretará la transferencia aludida en el punto VIII, o en su caso podrá exigirse la devolución parcial o total de la misma según corresponda.

Digitally signed by Gestion Documental Electronica
Date: 2021.06.15 14:07:59 -03:00

Jorge MENESES
Subsecretario
Subsecretaría de Contenidos Públicos
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2021.06.15 14:08:00 -03:00

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA

Resolución 9618/2021

RESOL-2021-9618-APN-SMYCP#JGM

Ciudad de Buenos Aires, 24/06/2021

VISTO los EX-2021-53459015--APN-DRRHHMYCP#JGM y EX-2021-39865715- -APN-DRRHHMYCP#JGM, los Decretos N°. 50 del 19 de diciembre de 2019, el Decreto N° 40 del 8 de enero de 2020, sus modificatorios y complementarios, y

CONSIDERANDO:

Que entre los objetivos asignados por el Poder Ejecutivo Nacional en el Decreto 50/19 sus modificatorios y complementarios, esta SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA se encuentra el de "(…) Fortalecer la libertad de expresión y la pluralidad cultural e informativa; e intervenir en acciones de vinculación del ESTADO NACIONAL con la ciudadanía, en el ámbito de su competencia (…)".

Que, asimismo, la SUBSECRETARÍA DE CONTENIDOS PÚBLICOS tiene entre sus objetivos el de "(…) Participar en la administración y funcionamiento de la formulación y ejecución de políticas de inclusión digital, con criterio federal en el ámbito de su competencia; gestionando a su vez, políticas públicas de promoción de contenidos para actores locales (…)".

Que, en esa línea esta Secretaría, en el marco del EX-2021-39865715- -APN-DRRHHMYCP#JGM ha propiciado el desarrollo de la página web SINERGIA (https://sinergia.jgm.gob.ar/), buscando generar un punto de encuentro entre el ESTADO NACIONAL y los medios de comunicación audiovisual de gestión social de la República Argentina.

Que el portal posee un espacio de capacitación a los fines de brindar herramientas para todas aquellas personas que, vinculadas a los medios de gestión social, deseen participar como productores de sentido en la circulación informativa en la sociedad.

Que, asimismo, la capacitación constituye una herramienta clave no sólo para desarrollar y/o potenciar la innovación y la productividad, sino además que permite mejorar el desempeño en la gestión de los medios de comunicación, a través de la generación de nuevos conocimientos que se traduzcan en mejores prácticas que fortalezcan y pluralicen la libertad de expresión e informativa.

Que, asociado a ello, resulta oportuno destacar la relación existente entre las políticas en materia de capacitación, con el estudio y análisis de las necesidades concretas de los medios de gestión social, permitiendo para tales fines, la formulación de desarrollos que coadyuven a incoar de manera eficiente las acciones estatales con las demandas genuinas del sector.

Que, por tal motivo, resulta imperioso establecer un programa que consista en la puesta en funcionamiento de un dispositivo de capacitación en pos de generar una estrategia de formación continua destinada a los actores de comunicación participantes de Medios de Gestión Social de todo el país.

Que la DIRECCIÓN TECNICO ADMINISTRATIVA DE MEDIOS Y COMUNICACIÓN PÚBLICA ha tomado la intervención de su competencia.

Que la DIRECCIÓN DE ASUNTOS LEGALES DE MEDIOS Y COMUNICACIÓN PÚBLICA ha tomado la intervención de su competencia.

Que la presente medida se dicta de conformidad con las atribuciones y facultades otorgada por el Decreto Nº 50/2019 y sus modificatorios y el Decreto 40/2020.

Por ello,

EL SECRETARIO DE MEDIOS Y COMUNICACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS

RESUELVE:

ARTICULO 1°. – Créase el PROGRAMA “SUMAR CAPACITACIÓN” con el objetivo principal de fortalecer la libertad de expresión, generando una mayor pluralidad cultural e informativa mediante la formación de los actores vinculados a los medios de gestión social de la República Argentina.

ARTÍCULO 2°. – Apruébense los lineamientos generales y acciones del PROGRAMA “SUMAR CAPACITACIÓN” que se encuentran en el ANEXO I registrado bajo el número IF-2021-53649652-APN-SSCPU#JGM que forma parte integrante de la presente.

ARTÍCULO 3°. – La SUBSECRETARÍA DE CONTENIDOS PÚBLICOS tendrá a su cargo el desarrollo de los mecanismos y procedimientos necesarios para la implementación del PROGRAMA creado en el ARTÍCULO 1º de la presente resolución, con intervención de las áreas técnicas pertinentes dependientes de la SUBSECRETARÍA DE GESTIÓN OPERATIVA DE MEDIOS PÚBLICOS.

ARTICULO 4°. – El gasto que demande la presente medida se atenderá con cargo a la Partida 5.1.4 – Ayudas sociales a personas, de la Categoría Programática 75 - Acciones para la federalización de la comunicación pública y de los contenidos, de este SAF 347 – Secretaría de Medios y Comunicación Pública.

ARTÍCULO 5°. - La presente Resolución entrará en vigencia el día de su publicación en el Boletín Oficial.

ARTÍCULO 6°. – Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL. Cumplido, archívese.

Juan Francisco Meritello

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 28/06/2021 N° 44298/21 v. 28/06/2021

Fecha de publicación 28/06/2021

EMERGENCIA PÚBLICA EN MATERIA OCUPACIONAL

Decreto 413/2021

DECNU-2021-413-APN-PTE - Prohibiciones de despidos y suspensiones. Prórroga.

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente N° EX-2021-54490896-APN-DGD#MT, la Ley N° 27.541, los Decretos Nros. 34 del 13 de diciembre de 2019, 156 del 14 de febrero de 2020, 260 del 12 de marzo de 2020, 297 del 19 de marzo de 2020, 329 del 31 de marzo de 2020, 367 del 13 de abril de 2020, 487 del 18 de mayo de 2020, 528 del 9 de junio de 2020, 624 del 28 de julio de 2020, 761 del 23 de septiembre de 2020, 891 del 13 de noviembre de 2020, 961 del 29 de noviembre de 2020, 39 del 22 de enero de 2021, 235 del 8 de abril de 2021, 266 del 21 de abril de 2021, 287 del 30 de abril de 2021, 334 del 21 de mayo de 2021, 345 del 27 de mayo de 2021 y 381 del 11 de junio de 2021, su respectiva normativa modificatoria y complementaria, y

CONSIDERANDO:

Que mediante el Decreto N° 34/19 se declaró la emergencia pública en materia ocupacional, la que fue ampliada por los Decretos N° 528/20, N° 961/20 y N° 39/21, hasta el 31 de diciembre de 2021.

Que por la Ley N° 27.541 se declaró la emergencia pública en materia económica, financiera, fiscal, administrativa, previsional, tarifaria, energética, sanitaria y social, la que posteriormente se dispuso ampliar en materia sanitaria a través del Decreto N° 260/20, en virtud de la pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con la COVID-19, por el plazo de UN (1) año; el que como consecuencia del agravamiento de la situación epidemiológica, fue prorrogado por el Decreto N° 167/21, hasta el 31 de diciembre de 2021.

Que, oportunamente, para hacer frente a la citada emergencia, a través del Decreto N° 297/20 se dispuso el “aislamiento social, preventivo y obligatorio” (ASPO), durante el plazo comprendido entre el 20 y el 31 de marzo de 2020, el que fue sucesivamente prorrogado mediante los Decretos Nros. 325/20, 355/20, 408/20, 459/20 y 493/20.

Que, posteriormente, por los Decretos Nros. 520/20, 576/20, 605/20, 641/20, 677/20, 714/20, 754/20, 792/20, 814/20, 875/20, 956/20, 1033/20, 67/21, 125/21 y 168/21 -cuya vigencia fue dejada sin efecto a partir del 9 de abril de 2021 por el Decreto N° 235/21- se fue diferenciando a las distintas áreas geográficas del país, entre aquellas que pasaron a una etapa de “distanciamiento social, preventivo y obligatorio” (DISPO) y aquellas que debieron retornar a la etapa de ASPO, en virtud de la evolución de la pandemia y de acuerdo al estatus sanitario de cada provincia, departamento y aglomerado, por sucesivos períodos.

Que luego, mediante los Decretos Nros. 235/21 y su modificatorio 241/21, y 287/21, prorrogado por sus similares Nros. 334/21 y 381/21, se establecieron medidas generales de prevención y disposiciones locales y focalizadas de contención, basadas en evidencia científica y en la dinámica epidemiológica, que deben cumplir todas las personas,

con el fin de mitigar la propagación del virus SARS-CoV-2 y su impacto sanitario, hasta el 25 de junio de 2021, inclusive.

Que, como se ha señalado reiteradamente, en el contexto descripto el Estado Nacional ha adoptado medidas de contención que tienen como objetivo ayudar a las empresas a sobrellevar los efectos de la emergencia, dictando como correlato necesario a las medidas de apoyo y sostén para el funcionamiento de las mismas medidas de tutela y protección de los puestos de trabajo, a través de los Decretos Nros. 329/20, 487/20, 624/20, 761/20, 891/20, 39/21, 266/21 y 345/21.

Que la segunda ola de COVID-19 que azota al país debe ser acompañada por medidas acordes que contemplen la protección de la salud de la población y coadyuven a morigerar el impacto de las medidas sanitarias sobre el empleo.

Que mediante el Mensaje N° 48 del 10 de mayo de 2021, el PODER EJECUTIVO NACIONAL envió al HONORABLE CONGRESO DE LA NACIÓN un Proyecto de Ley por el cual se proponen indicadores precisos para establecer el nivel de riesgo epidemiológico y sanitario de cada zona del país, con el fin de establecer un modelo que otorgue previsibilidad al determinar las acciones y medidas que regirán ante el riesgo creciente.

Que la protección preferente de las trabajadoras y los trabajadores es una garantía que la CONSTITUCIÓN NACIONAL incluye en el artículo 14 bis y que, en idéntico sentido, normas internacionales incorporadas en el artículo 75, inciso 22, obligan a adoptar medidas robustas de mayor intensidad en contextos excepcionales que ponen en riesgo el propio tejido del sistema de relaciones laborales.

Que, en función de ello, es necesario acompañar las medidas de emergencia prorrogando la adopción de aquellas que resguardan los puestos de trabajo, como herramientas de política laboral necesarias para la protección de las trabajadoras y los trabajadores, asegurándoles que esta crisis excepcional no les hará perder sus puestos de trabajo.

Que la ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (O.I.T.) ha emitido un documento denominado “Las normas de la OIT y la COVID-19 (coronavirus)” que revela la preocupación mundial y alude a la necesidad de que los gobiernos implementen medidas dirigidas a paliar los efectos nocivos en el mundo del trabajo, en particular en lo referido a la conservación de los puestos de labor y en tal sentido recuerda la importancia de tener presente la Recomendación 166, que subraya “que todas las partes interesadas deberían tratar de evitar o limitar en todo lo posible la terminación de la relación de trabajo por motivos económicos, tecnológicos, estructurales o análogos, sin perjuicio para el funcionamiento eficaz de la empresa, establecimiento o servicio, y esforzarse por atenuar las consecuencias adversas de toda terminación de la relación de trabajo por estos motivos, para el trabajador o los trabajadores interesados”.

Que, asimismo, el mencionado organismo ha llevado a cabo un análisis pormenorizado sobre las disposiciones fundamentales de las normas internacionales del trabajo pertinentes en el contexto del brote de la COVID-19, publicado el 27 de marzo de 2020, sosteniendo que las patologías contraídas por exposición en el trabajo a dicho agente patógeno podrían considerarse como enfermedades profesionales.

Que, en ese marco, diversos países han declarado que la afección por la COVID-19 producida por la exposición de los trabajadores y las trabajadoras al virus SARS-CoV-2 durante la realización de sus tareas laborales, reviste carácter de enfermedad profesional.

Que en nuestro país, mediante el artículo 6º del Decreto Nº 345/21 se prorrogó hasta el 30 de junio de 2021, inclusive, lo dispuesto por el artículo 7° del Decreto Nº 39/21 -por el cual se estableció que por un plazo determinado la enfermedad COVID-19 producida por el virus SARS-CoV-2 será considerada presuntivamente una enfermedad de carácter profesional (no listada)-, respecto de la totalidad de las trabajadoras y los trabajadores dependientes incluidas e incluidos en el ámbito de aplicación personal de la Ley N° 24.557 sobre Riesgos del Trabajo que hayan prestado efectivamente tareas en sus lugares de trabajo.

Que subsistiendo las causas que motivaron aquella medida, corresponde prorrogar los términos de la misma.

Que las medidas que se establecen en el presente decreto son razonables y proporcionadas con relación a la amenaza y al riesgo sanitario que enfrenta nuestro país y se adoptan en forma temporaria, toda vez que resultan perentorias y necesarias para proteger la salud de determinados sectores de la población trabajadora particularmente vulnerable.

Que la Ley N° 26.122 regula el trámite y los alcances de la intervención del HONORABLE CONGRESO DE LA NACIÓN respecto de los Decretos de Necesidad y Urgencia dictados por el PODER EJECUTIVO NACIONAL en virtud de lo dispuesto por el artículo 99, inciso 3 de la CONSTITUCIÓN NACIONAL.

Que la citada ley determina que la COMISIÓN BICAMERAL PERMANENTE tiene competencia para pronunciarse respecto de la validez o invalidez de los Decretos de Necesidad y Urgencia, así como para elevar el dictamen al plenario de cada Cámara para su expreso tratamiento, en el plazo de DIEZ (10) días hábiles.

Que el artículo 22 de la Ley N° 26.122 dispone que las Cámaras se pronuncien mediante sendas resoluciones, y que el rechazo o aprobación de los decretos deberá ser expreso conforme lo establecido en el artículo 82 de la Carta Magna.

Que ha tomado intervención el servicio jurídico competente.

Que la presente medida se dicta en uso de las atribuciones conferidas por el artículo 99, incisos 1 y 3 de la CONSTITUCIÓN NACIONAL.

Por ello,

EL PRESIDENTE DE LA NACIÓN ARGENTINA EN ACUERDO GENERAL DE MINISTROS

DECRETA:

ARTÍCULO 1°.- El presente decreto se dicta en el marco de la emergencia pública en materia sanitaria declarada por la Ley N° 27.541, ampliada por el Decreto N° 260/20, sus modificatorios y su prórroga establecida por el Decreto N° 167/21 y la emergencia pública en materia ocupacional declarada por el Decreto Nº 34/19 y ampliada

por sus similares Nros. 528/20, 961/20 y 39/21.

ARTÍCULO 2°.- Prorrógase hasta el 31 de diciembre de 2021 inclusive, la prohibición de efectuar despidos sin justa causa y por las causales de falta o disminución de trabajo y fuerza mayor, dispuesta por el artículo 2° del Decreto N° 329/20 y sus sucesivas prórrogas.

ARTÍCULO 3°.- Prorrógase hasta el 31 de diciembre de 2021, inclusive, la prohibición de efectuar suspensiones por las causales de fuerza mayor o falta o disminución de trabajo, dispuesta por el artículo 3° del Decreto N° 329/20 y sus sucesivas prórrogas.

Quedan exceptuadas de esta prohibición y de los límites temporales previstos por los artículos 220, 221 y 222 de la Ley de Contrato de Trabajo N° 20.744 (t.o. 1976) y sus modificatorias, las suspensiones efectuadas en los términos del artículo 223 bis de la misma, como consecuencia de la emergencia sanitaria.

ARTÍCULO 4°.- Los despidos y las suspensiones que se dispongan en violación de lo dispuesto en el artículo 2° y en el primer párrafo del artículo 3º del presente decreto, no producirán efecto alguno y se mantendrán vigentes las relaciones laborales existentes y sus condiciones actuales.

ARTÍCULO 5°.- Las prohibiciones previstas en el presente decreto no serán aplicables a las contrataciones celebradas con posterioridad a la entrada en vigencia del Decreto N° 34/19, ni respecto del personal que preste servicios en el ámbito del Sector Público Nacional definido en el artículo 8° de la Ley N° 24.156 y sus modificatorias, con independencia del régimen jurídico al que se encuentre sujeto y de la naturaleza jurídica de la entidad empleadora.

Quedan asimismo exceptuados y/o exceptuadas de tales prohibiciones, quienes se encuentren comprendidos y/o comprendidas en el régimen legal de trabajo para el personal de la industria de la construcción regulado por la Ley Nº 22.250.

ARTÍCULO 6º.- Prorrógase hasta el 31 de diciembre de 2021, inclusive, lo dispuesto por el artículo 7° del Decreto Nº 39/21 prorrogado por el artículo 6º del Decreto Nº 345/21, respecto de la totalidad de las trabajadoras y los trabajadores dependientes incluidas e incluidos en el ámbito de aplicación personal de la Ley N° 24.557 sobre Riesgos del Trabajo y que hayan prestado efectivamente tareas en sus lugares habituales, fuera de su domicilio particular.

Serán de aplicación a su respecto las normas contenidas en los artículos 2° y 3° del Decreto N° 367/20.

El financiamiento de estas prestaciones será imputado al FONDO FIDUCIARIO DE ENFERMEDADES PROFESIONALES creado mediante el Decreto N° 590/97 de acuerdo a las regulaciones que dicte la SUPERINTENDENCIA DE RIESGOS DEL TRABAJO y deberá garantizarse el mantenimiento de una reserva mínima equivalente al DIEZ POR CIENTO (10 %) de los recursos de este último, con el objeto de asistir el costo de cobertura prestacional de otras posibles enfermedades profesionales, según se determine en el futuro.

ARTÍCULO 7º.- El presente decreto entrará en vigencia a partir del día de su publicación en el BOLETÍN OFICIAL.

ARTÍCULO 8º.- Dese cuenta a la COMISIÓN BICAMERAL PERMANENTE del HONORABLE CONGRESO DE LA NACIÓN.

ARTÍCULO 9º.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

FERNÁNDEZ - Santiago Andrés Cafiero - Eduardo Enrique de Pedro - Agustin Oscar Rossi - Martín Guzmán - Matías Sebastián Kulfas - Alexis Raúl Guerrera - Gabriel Nicolás Katopodis - Luis Eugenio Basterra - Martín Ignacio Soria - Sabina Andrea Frederic - Carla Vizzotti - Daniel Fernando Arroyo - Elizabeth Gómez Alcorta - Nicolás A. Trotta - Tristán Bauer - Roberto Carlos Salvarezza - Claudio Omar Moroni - Juan Cabandie - Matías Lammens - Jorge Horacio Ferraresi - E/E Agustin Oscar Rossi

e. 28/06/2021 N° 44527/21 v. 28/06/2021

Fecha de publicación 28/06/2021

SECTOR PÚBLICO NACIONAL

Decisión Administrativa 641/2021

DECAD-2021-641-APN-JGM - Requisitos mínimos de Seguridad de la Información para Organismos.

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente No EX-2021-00877103-APN-SIP#JGM, la Ley de Ministerios (texto ordenado por Decreto N° 438 del 12 de marzo de 1992 y sus modificatorias), la Ley N° 24.156 y sus modificatorias, los Decretos Nros. 577 del 28 de julio de 2017 y su modificatorio, 50 del 19 de diciembre de 2019 y sus modificatorios, las Decisiones Administrativas Nros. 669 del 20 de diciembre de 2004 y su modificatoria y 1865 del 14 de octubre de 2020, las Resoluciones de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN Nros. 829 del 24 de mayo de 2019 y 1523 del 12 de septiembre de 2019 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1 del 19 de febrero de 2015, y

CONSIDERANDO:

Que por la Decisión Administrativa N° 669/04 se estableció que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias debían dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

Que por el Decreto N° 577/17 modificado por su similar N° 480 del 11 de julio de 2019 se creó el COMITÉ DE CIBERSEGURIDAD en la órbita de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, el cual tiene por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

Que, asimismo, por el citado decreto se encomendó a la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN o a quien esta designara, impulsar los actos administrativos y demás acciones necesarias para la implementación de la Estrategia Nacional de Ciberseguridad que apruebe el COMITÉ DE CIBERSEGURIDAD, así como de los objetivos en ella contenidos.

Que dentro de este marco normativo, por la Resolución N° 829/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN se aprobó la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD y se creó, en el marco del referido COMITÉ DE CIBERSEGURIDAD y en la órbita de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, la Unidad Ejecutiva, cuyas funciones se consignan en el ANEXO II de esa medida.

Que por la Resolución N° 1523/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN se aprobó la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

Que la resolución citada en el considerando anterior define a las Infraestructuras Críticas como aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Que, de igual modo, la mencionada resolución determina como Infraestructuras Críticas de Información a aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

Que se ha producido en los últimos años un incremento sustancial en el uso de las Tecnologías de la Información y las Comunicaciones en el ámbito del Sector Público Nacional, al punto de que se han tornado indispensables para el desenvolvimiento de toda la actividad de las entidades y jurisdicciones que lo componen, tanto en lo que se refiere a la gestión interna como a los servicios que prestan a la sociedad.

Que el intenso uso de las Tecnologías de la Información y las Comunicaciones conlleva asimismo un notable aumento de los riesgos y amenazas a los activos de información y a los sistemas esenciales utilizados para brindar de manera eficiente y constante los múltiples servicios que desde el Sector Público Nacional se prestan.

Que las nuevas formas de ataques informáticos y la actividad maliciosa en general avanzan y se modifican en forma vertiginosa, obligando a mantener actualizadas las herramientas, protocolos y marcos normativos, con el fin de proteger adecuadamente la infraestructura, los activos de información y principalmente los datos personales, que son en definitiva un patrimonio de los ciudadanos en su conjunto.

Que resulta necesario avanzar en el proceso de fortalecimiento de la seguridad de la información que reciben, producen y administran las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, con el fin de dotarlas de las características de confidencialidad, integridad y disponibilidad.

Que por lo expuesto, y atento al incremento, cantidad y variedad de amenazas y vulnerabilidades que rodean a los activos de información, corresponde derogar la Decisión Administrativa N° 669/04 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1/15 -por la que oportunamente se aprobara la “Política de Seguridad de la Información Modelo”-, puesto que las mismas han perdido virtualidad y no reflejan en forma apropiada la situación actual en la materia ni sientan las bases normativas que permitan mantener adecuadamente actualizados los niveles de seguridad de la información que ingresa, y la que generan y producen las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias.

Que si bien la referida Decisión Administrativa N° 669/04 consideraba en el alcance de la norma a las entidades comprendidas en los incisos a) y c) del artículo 8° de la ley citada precedentemente, debido a las características que revisten los requisitos mínimos exigidos se ha considerado más apropiado acotar el alcance de la presente medida a los organismos pertenecientes a la Administración Central y a aquellos descentralizados.

Que, asimismo, la información puede ser objeto de una amplia gama de usos indebidos, debiéndose preservar su confidencialidad, integridad y disponibilidad, con el fin de garantizar la prestación continua e ininterrumpida de los diversos servicios prestados por el Sector Público Nacional.

Que, en este marco, se torna necesario que cada entidad y jurisdicción del Sector Público Nacional comprendida en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias sea capaz de prevenir que sus sistemas de información se vean afectados, implementando, a tal fin, un Plan de Seguridad.

Que a tales fines es indispensable determinar una serie de requisitos mínimos de seguridad para el tratamiento de los datos y los activos de información que gestionan las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, con el fin de adecuarlos a las buenas prácticas y estándares nacionales e internacionales, que contemple tanto la ampliación y profundización en el uso del espacio digital como la emergencia de las nuevas amenazas y riesgos para la confidencialidad, integridad y disponibilidad de la información.

Que, en consecuencia, a los efectos de facilitar la elaboración y ejecución de los Planes de Seguridad mencionados y elevar, a la par, los niveles de seguridad de los sistemas de información de las entidades y jurisdicciones del Sector Público Nacional comprendidos en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, deviene necesario aprobar los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” y establecer todos aquellos recaudos complementarios necesarios.

Que en función de lo expresado es necesario que cada una de las entidades y jurisdicciones del Sector Público Nacional comprendida en el inciso a) del artículo 8° de la Ley N° 24.156 y sus modificatorias asuma la obligación de proteger adecuadamente la información que gestiona, a través de la urgente adopción de medidas preventivas, detectivas y correctivas específicas, destinadas a proteger dicha información y recursos, de conformidad con sus competencias y funciones y en concordancia con los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL”.

Que, consecuentemente, deviene indispensable que cada entidad y jurisdicción alcanzada por la presente decisión administrativa, en el marco del Plan de Seguridad que apruebe y a los fines del cumplimiento de los requisitos de seguridad, apruebe una Política de Seguridad de la Información.

Que la Ley de Ministerios (texto ordenado por Decreto N° 438 del 12 de marzo de 1992 y sus modificatorias) establece entre las atribuciones del Jefe de Gabinete de Ministros la de “Entender en el diseño y ejecución de políticas relativas al empleo público, a la innovación de gestión, a la modernización de la Administración Pública Nacional, al régimen de compras y contrataciones, a las tecnologías de la información, las telecomunicaciones, los servicios de comunicación audiovisual y los servicios postales”.

Que por el Decreto Nº 139 del 4 de marzo de 2021 se incorporó a las funciones que el Decreto N° 50/19 le asignaba a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, el

objetivo de “Entender en la ciberseguridad y protección de infraestructuras críticas de información y comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078”.

Que, asimismo, por el Decreto N° 139/21 antes mencionado se establece además como función de la SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES de la SECRETARÍA DE INNOVACIÓN PÚBLICA, la de “Proponer a la Secretaría estrategias, estándares y regulaciones para la ciberseguridad y protección de infraestructuras críticas de la información y las comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078”.

Que a través de la Decisión Administrativa Nº 1865/20 se aprobó la estructura organizativa del primer y segundo nivel operativo de la JEFATURA DE GABINETE DE MINISTROS, estableciendo como Responsabilidad Primaria de la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA la de “Entender en todos los aspectos relativos a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional”.

Que, asimismo, la mencionada decisión administrativa definió, entre las acciones de la citada DIRECCIÓN NACIONAL DE CIBERSEGURIDAD, las de: diseñar políticas de ciberseguridad, en coordinación con los organismos del ESTADO NACIONAL con competencia en la materia; elaborar planes, programas y proyectos con perspectiva federal en materia de ciberseguridad, en el ámbito de competencia de la Secretaría; participar en las acciones destinadas a implementar los objetivos fijados en la Estrategia Nacional de Ciberseguridad, articulando proyectos con las diferentes áreas del ESTADO NACIONAL involucradas y proponer proyectos de normas relacionados con la ciberseguridad en la REPÚBLICA ARGENTINA, en coordinación con las áreas con competencia en la materia.

Que en este marco resulta pertinente el dictado de un acto administrativo que contribuya a que paulatinamente se incorporen controles que permitan una gestión más responsable, segura y transparente de la información que es tratada por ciertas áreas del Sector Público Nacional.

Que han tomado la intervención de su competencia los servicios jurídicos pertinentes.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 100, inciso 1 de la CONSTITUCIÓN NACIONAL.

Por ello,

EL JEFE DE GABINETE DE MINISTROS

DECIDE:

ARTÍCULO 1°.- Apruébanse los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” que como ANEXO I (IF-2021-50348419-APN-SSTIYC#JGM) forman parte integrante de la presente medida.

ARTÍCULO 2°.- La presente decisión administrativa será de aplicación a las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias y a los proveedores que contraten con esas entidades y jurisdicciones, en todo aquello que se encuentre relacionado con las tareas que realicen y en los términos que establezca cada una de ellas, normativa o contractualmente.

ARTÍCULO 3°.- Las entidades y jurisdicciones del Sector Público Nacional comprendidas en el artículo 2° de esta medida deberán aprobar sus Planes de Seguridad en el plazo máximo de NOVENTA (90) días desde la entrada en vigencia de la presente. Dichos Planes de Seguridad deberán establecer los plazos en que se dará cumplimiento a cada uno de los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” establecidos en el ANEXO I de la presente; plazo que no podrá ser posterior al 31 de diciembre de 2022.

ARTÍCULO 4°.- Los Planes de Seguridad mencionados en el artículo 3° deberán ser remitidos a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA, dependiente de la JEFATURA DE GABINETE DE MINISTROS y/o a la que en el futuro la reemplace, dentro de un plazo máximo de NOVENTA (90) días desde la entrada en vigencia de la presente.

ARTÍCULO 5°.- Las máximas autoridades de las entidades y jurisdicciones comprendidas en el artículo 2° de la presente deberán asignar las funciones relativas a la seguridad de sus sistemas de información al área con competencia en la materia e informar, mediante Comunicación Oficial a través del Sistema de Gestión Documental Electrónica (GDE) a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS el nombre, apellido y datos de contacto del responsable del área designada, dentro del plazo de SESENTA (60) días corridos desde la entrada en vigencia de la presente medida.

ARTÍCULO 6°.- Las entidades y jurisdicciones comprendidas en el artículo 2° de esta medida deberán adoptar las medidas preventivas, detectivas y correctivas destinadas a proteger la información que reciban, generen o gestionen como asimismo sus recursos.

ARTÍCULO 7°.- Las entidades y jurisdicciones establecidas en el artículo 2° de la presente medida deberán reportar a la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS los incidentes de seguridad que se produzcan dentro de sus ámbitos, dentro de las CUARENTA Y OCHO (48) horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.

ARTÍCULO 8°.- Encomiéndase a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS o a quien esta designe, la revisión y actualización periódica de los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL”, como

asimismo el dictado de las normas complementarias y aclaratorias de la presente medida.

ARTÍCULO 9°.- Deróganse la Decisión Administrativa N° 669 del 20 de diciembre de 2004 y la Disposición de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN N° 1 del 19 de febrero de 2015.

ARTÍCULO 10.- Invítase a las entidades y jurisdicciones enumeradas en los incisos b), c) y d) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias, a los Gobiernos Provinciales, de la Ciudad Autónoma de Buenos Aires y Municipales, y a los Poderes Legislativo y Judicial de la Nación a adherir a la presente.

ARTÍCULO 11.- La DIRECCIÓN NACIONAL DE CIBERSEGURIDAD de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS verificará el cumplimiento de las disposiciones de la presente medida, sin perjuicio de las competencias asignadas a la SINDICATURA GENERAL DE LA NACIÓN.

ARTÍCULO 12.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Santiago Andrés Cafiero - Eduardo Enrique de Pedro

NOTA: El/los Anexo/s que integra/n este(a) Decisión Administrativa se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 28/06/2021 N° 44521/21 v. 28/06/2021

Fecha de publicación 28/06/2021

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Anexo

Número: IF-2021-50348419-APN-SSTIYC#JGM

CIUDAD DE BUENOS AIRES
Viernes 4 de Junio de 2021

Referencia: ANEXO I - REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SPN

ANEXO I

REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN [1]

PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL

I. INTRODUCCIÓN

Los organismos del Sector Público Nacional comprendidos en el artículo 8º de la Ley Nº 24.156 y sus modificatorias son de los principales receptores y productores de información de nuestro país. Esa información pertenece mayormente a sus habitantes y a las diversas entidades públicas y privadas que desarrollan sus actividades en su territorio. Todos ellos confían sus datos a los organismos que lo componen para distintos fines.

La información puede ser hoy en día objeto de una amplia gama de peligros, amenazas y usos indebidos e ilícitos, debiéndose, por lo tanto, extremar las medidas tendientes a la preservación de su confidencialidad, integridad y disponibilidad. Con esto se busca proteger los derechos y libertades individuales de las personas al tiempo de contribuir a la efectiva prestación continua e ininterrumpida de los diversos servicios prestados por las diferentes entidades y jurisdicciones y, al mismo tiempo, propender a su correcta y mejor gestión interna.

En un contexto de transversalidad en el uso de las tecnologías para la vida social, económica, política y cultural de las personas, la seguridad de la información cumple un rol fundamental. Por consiguiente, los agentes públicos, cualquiera sea el nivel jerárquico y la modalidad de contratación, tienen la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos.

Los responsables de los activos de la información deben atender y diligenciar los recursos necesarios para asegurar el cumplimiento de los objetivos de la presente en el ámbito de su jurisdicción. En tal sentido, los datos gestionados en los organismos deben ser protegidos tanto dentro como fuera del ámbito institucional, con independencia del formato y del soporte en el que estén contenidos y si los mismos están siendo objeto de tratamiento electrónico, se encuentran almacenados o están siendo transmitidos.

Los organismos determinarán sus políticas, normas específicas, procedimientos y guías que, sobre la base de los siguientes requisitos mínimos, sean aplicables a los procesos específicos que desarrollen. Este conjunto de normas debe surgir a partir de un análisis de los riesgos para los procesos que lleven adelante.

Se entenderán como principios de seguridad de la información a la preservación de confidencialidad, integridad y disponibilidad de la información y de los activos de información del Sector Público Nacional.

II. OBJETIVOS

Objetivo general

Establecer los lineamientos generales y mínimos para los organismos del Sector Público Nacional comprendidos en el inciso a) del artículo 8º de la Ley Nº 24.156, con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

Objetivos específicos

- Proteger los derechos de los titulares de datos personales o propietarios de información que es tratada por el Sector Público Nacional.
- Proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional.
- Promover una política pública que enmarque una conducta responsable en materia de seguridad de la información de los organismos que conforman el Sector Público Nacional, sus agentes y funcionarios.
- Evidenciar el compromiso e interés de quienes componen el Sector Público Nacional en pos del desarrollo de una cultura de ciberseguridad.

III. ALCANCE

Las directrices que surgen de los presentes requisitos mínimos de seguridad serán de aplicación obligatoria para todos los agentes y funcionarios que se desempeñan en los organismos que componen el Sector Público Nacional según el inciso a) del artículo 8º de la Ley Nº 24.156 y sus modificatorias, en la medida que les corresponda según su función. Las autoridades máximas de los organismos públicos serán las responsables de proveer los medios necesarios para su efectivo cumplimiento y de promover su utilización.

En el caso de los entes reguladores que estén comprendidos dentro del artículo 8º de la Ley Nº 24.156 y sus modificatorias, se recomienda el análisis de una eventual incorporación de los principios de la Seguridad de la

Información. Asimismo, se sugiere la evaluación de la oportunidad y pertinencia de establecer requisitos mínimos de seguridad de la información que más adelante se detallan en la sección V. Directrices, para el sector regulado.

El cumplimiento de los presentes requisitos mínimos de seguridad será también exigible a los terceros que contraten con el Sector Público Nacional, en las secciones que sean aplicables a las tareas que realizan y en los términos que establezca cada organismo en sus disposiciones normativas y contractuales.

IV. REVISIÓN Y ACTUALIZACIÓN

Los requisitos mínimos de Seguridad serán revisados por la Dirección Nacional de Ciberseguridad de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, o el área que la reemplace en el futuro, cuando lo estime conveniente, con una periodicidad no superior a DOCE (12) meses, a partir de su publicación o última actualización. Serán publicados también en el sitio de Internet que, a tal fin, establezca la Dirección Nacional antes citada.

V. DIRECTRICES

1. Política de Seguridad de la Información del organismo

Los organismos deben desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlos. Los términos de dicha política deben ser consistentes con las directrices del presente documento.

Dicha política debe ser:

- aprobada por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.
- notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.
- cumplida por todos los agentes y funcionarios del organismo.
- revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.
- utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.
- informada a la Dirección Nacional de Ciberseguridad una vez aprobada.

2. Aspectos Organizativos de la Seguridad

Se debe desarrollar e implementar un marco organizativo que habilite una efectiva gestión y operación de la seguridad de la información en el organismo.

Esto implica que se debe:

- asignar a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información, incluyendo el cumplimiento de las directrices del presente documento. Se

deberá informar a la Dirección Nacional de Ciberseguridad el nombre y datos de contacto del responsable del área a la que se le han asignado las funciones y mantener dichos datos actualizados.

- segregar las funciones y áreas de responsabilidad en conflicto para incrementar los niveles de seguridad de la información. En la medida de lo posible, se recomienda que las funciones de seguridad de la información no dependan del área de Sistemas o Tecnología de la Información.
- impulsar desde el mayor nivel jerárquico las iniciativas que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona.
- abordar los aspectos referidos a la seguridad de la información en el diseño y la gestión de todos los proyectos que lleve adelante el organismo, dejando evidencia de tal intervención.
- establecer como falta, sobre la base del régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias, el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, por parte de los agentes y funcionarios, incluyendo una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.
- incluir en los contratos, Términos de Referencia o en el instrumento mediante el cual se materialice la contratación del personal que se emplee bajo las modalidades que correspondan, cláusulas que contemplen el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, incluyendo una graduación en las responsabilidades y sanciones que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.
- establecer mecanismos adecuados de seguridad para el trabajo remoto y para el uso de dispositivos móviles, sean estos provistos por el organismo o propiedad de agentes y funcionarios, según la criticidad de la información involucrada y del nivel jerárquico del funcionario.

3. Seguridad Informática de los Recursos Humanos

Los organismos deben adoptar una perspectiva sistémica para proteger sus activos de información, dentro de la cual el personal debe ser considerado un recurso central. Asimismo, deben establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad. Los agentes y funcionarios deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos.

Para ello será necesario:

- realizar e implementar planes de concientización en el uso seguro y responsable de los activos de información, que incluyan capacitaciones periódicas destinadas a todos los agentes y funcionarios del organismo, diseñándolos para cada tipo de público y con distintas temáticas.
- promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.
- establecer la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información para todos los empleados del organismo, cualquiera sea su modalidad de contratación, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.
- establecer claramente los requerimientos de seguridad de la información, que incluya niveles de acceso a la

información para cada perfil de trabajo.
- incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.
- requerir a los agentes y funcionarios, cuando el organismo lo considere necesario, de acuerdo a sus competencias, la firma de un acuerdo de confidencialidad.
- incorporar dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo.

4. Gestión de Activos

Los activos de información del organismo deben ser gestionados y protegidos en forma efectiva. En el mismo sentido, deben ser clasificados según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, teniendo en cuenta sus funciones, la normativa que les sea aplicable y cualquier otro activo que pudieran contener de otros organismos públicos o entidades privadas, lo que permitirá adoptar las medidas de protección adecuadas.

Para ello se requiere:

- clasificar los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.
- llevar un inventario actualizado en el que se detallen los datos necesarios para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.
- exigir a todos los agentes y empleados la devolución de los activos de información en su poder al finalizar la relación laboral o cuando un cambio en las funciones lo requiera.
- efectuar una destrucción segura de cualquier medio que pueda contener información o datos personales, en función de su nivel de criticidad, sobre la base de un procedimiento documentado, una vez que se haya catalogado como defectuoso o rezago.

5. Autenticación, Autorización y Control de Accesos

El acceso a los activos de información del organismo debe realizarse a partir de procesos y mecanismos de seguridad definidos e implementados según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. Los privilegios de acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones.

En consiguiente se debe:

- utilizar en todos los casos el principio de “necesidad de saber”, es decir que solo se otorguen privilegios de acceso en la medida en que sean requeridos para las actividades y tareas que cada empleado o funcionario debe llevar adelante.
- hacer una adecuada y oportuna gestión de las altas y bajas de cuentas de usuario y privilegios, coordinando con las áreas de Recursos Humanos y aquellas en las que el empleado se desempeña toda novedad que pudiera impactar en ellos.
- realizar un seguimiento detallado sobre las cuentas con privilegios especiales.
- revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.
- requerir a los agentes, funcionarios y demás usuarios un uso responsable de sus dispositivos y datos de autenticación, dejando sentado que se encuentra estrictamente prohibido compartirlos y que deben ser mantenidos seguros en forma permanente.

- restringir y controlar la asignación y uso de derechos de accesos privilegiados.
- limitar y monitorear el acceso al código fuente de los programas.

6. Uso de herramientas criptográficas

La confidencialidad, integridad, autenticidad y/o no repudio de la información del organismo debe ser protegida mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.

En este marco se debe:

- requerir el cifrado de cualquier dispositivo del organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.
- proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.
- utilizar certificados digitales en todos los sitios de Internet del organismo.

7. Seguridad física y ambiental

Los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.

Esto implica:

- la identificación y protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales.
- la incorporación de controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.
- el registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.
- la adopción de medidas de seguridad para que el equipamiento sea ingresado o retirado del organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.
- el cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.
- la adopción de medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del organismo y la interrupción de sus operaciones.
- la protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.
- el mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continuas.
- la adopción de medidas de seguridad para los activos informáticos que deben llevarse fuera del organismo, considerando los distintos riesgos de trabajar fuera de sus dependencias, en lo que hace al resguardo de la información y a la seguridad física de los dispositivos.

8. Seguridad operativa

Las operaciones del organismo deben desarrollarse en forma segura, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para ello se debe:

- establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.
- revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.
- minimizar los riesgos de acceso o de cambios no autorizados en entornos productivos, separando los entornos de desarrollo, prueba y producción, en los casos que corresponda.
- implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.
- proteger las instalaciones contra infecciones de código malicioso.
- realizar copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.
- llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes.
- mantener un control estricto sobre el software y su integridad, en entornos productivos.
- identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación.
- gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.
- registrar y revisar periódicamente las actividades de los administradores y operadores.

9. Seguridad en las comunicaciones

La información de las redes del organismo debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.

Se debe:

- Segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.
- proteger adecuadamente la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.
- exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.
- incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.

10. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites

a través de Internet.

Para ello se debe:

- especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.
- utilizar una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.
- controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción e incorporando efectivos controles cruzados o por oposición.
- proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.
- utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.
- evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.
- proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.
- controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el cocontratante en aquellas contrataciones de bienes y servicios efectuadas por el organismo.

11. Relación con proveedores

La contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio debe incluir en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del cocontratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

Esto comprende:

- la consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.
- el establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al organismo.
- la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.
- la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.
- la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.

12. Gestión de incidentes de seguridad

El organismo debe adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

Para ello debe:

- identificar las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.
- contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.
- adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.
- instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.
- notificar a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.
- recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.
- en el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.

13. Aspectos de seguridad para la continuidad de la gestión

Los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales deben contemplar todos los aspectos de seguridad de la información involucrada.

Para ello se debe:

- identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.
- establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.
- verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.
- implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

14. Cumplimiento

En todos los casos el organismo debe cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.

Esto implica:

- la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.

- el cumplimiento de la Ley Nº 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.
- la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.
- la supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.
- considerar la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.

VI. Glosario

Los términos utilizados en este documento se encuentran incluidos en el Glosario aprobado por la Resolución N° 1523/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN y en la Ley Nº 25.326 de Protección de los Datos Personales.

---

[1] Para la elaboración del presente documento se han tomado como referencia estándares nacionales e internacionales reconocidos, tales como las Normas IRAM-ISO/IEC 27001, 27002 y 20000-1.

Digitally signed by Gestion Documental Electronica
Date: 2021.06.04 18:04:28 -03:00

Martín OLMOS
Subsecretario
Subsecretaría de Tecnologías de la Información y las Comunicaciones
Jefatura de Gabinete de Ministros

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO

Resolución 62/2021

RESOL-2021-62-APN-SGYEP#JGM

Ciudad de Buenos Aires, 25/06/2021

VISTO el Expediente N° EX-2021-56258684- -APN-SGYEP#JGM, del Registro de la JEFATURA DE GABINETE DE MINISTROS, las Leyes Nº 27.491, N° 27.541 y sus modificatorios y N° 27.573, los Decretos N° 260 del 12 de marzo de 2020 y sus modificatorios y N° 287 del 30 de abril de 2021 y sus modificatorios, la Decisión Administrativa Nº 390 del 16 de marzo de 2020 y su modificatoria, las Resoluciones del MINISTERIO DE SALUD N° 627 del 19 de marzo del 2020 y su modificatoria y N° 2883 del 29 de diciembre de 2020, la Resolución Conjunta del MINISTERIO DE SALUD y el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL Nº 4 del 8 de abril de 2021, y

CONSIDERANDO:

Que mediante la Ley de Solidaridad Social y Reactivación Productiva N° 27.541 se declaró la emergencia pública en materia económica, financiera, fiscal, administrativa, previsional, tarifaria, energética, sanitaria y social.

Que, posteriormente, a través del Decreto N° 260 del 12 de marzo de 2020 y sus modificatorios se amplió la emergencia pública en materia sanitaria con motivo de la pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el nuevo coronavirus COVID-19 por el plazo de UN (1) año desde su entrada en vigencia, el cual fue prorrogado por el Decreto Nº 167 del 11 de marzo de 2021 hasta el día 31 de diciembre de 2021, y se facultó al MINISTERIO DE SALUD DE LA NACIÓN a adoptar las medidas que resulten oportunas y necesarias para la prevención de la propagación del SARS-CoV-2, con el objeto de minimizar sus efectos e impacto sanitario.

Que, ante la actual situación epidemiológica y el acelerado aumento de casos, mediante el Decreto Nº 287 del 30 de abril de 2021 y sus modificatorios se implementó la clasificación de las situaciones de riesgo epidemiológico, asociadas con medidas temporarias, intensivas, focalizadas geográficamente y orientadas a las actividades y horarios que conllevan mayores riesgos, que incluyeron a las organizaciones y las y los trabajadores del Sector Público.

Que la norma mencionada en el párrafo anterior, se encuentra vigente y prorrogada por el Decreto N° 381 del 11 de junio de 2021.

Que, sin perjuicio de lo anterior, cabe destacar que por Ley N° 27.491 se declaró la vacunación de interés nacional, entendiéndosela como una estrategia de salud pública preventiva y altamente efectiva, y considerándosela como un bien social, sujeto a principios de gratuidad, interés colectivo, disponibilidad y amplia participación.

Que contar con una vacuna segura y eficaz para prevenir el COVID-19 es determinante para controlar el avance de la enfermedad, ya sea disminuyendo la morbimortalidad o la transmisión del virus, y permite mejorar el cuidado de la vida y la salud de los y las habitantes del país, así como restablecer paulatinamente las actividades económicas y sociales.

Que por Resolución del MINISTERIO DE SALUD N° 2883 del 29 de diciembre de 2020 se aprobó el “Plan Estratégico para la Vacunación contra la COVID-19 en la República Argentina”, el cual establece una estrategia de vacunación voluntaria, escalonada y en etapas no excluyentes, procurando ampliar progresivamente la población objetivo y permitiendo inmunizar de forma gradual a mayor cantidad de personas.

Que el Estado Nacional suscribió diversos acuerdos tendientes a la adquisición de vacunas en tiempo oportuno, lo cual permitió iniciar la vacunación en las VEINTICUATRO (24) jurisdicciones del país de manera simultánea en el mes de diciembre pasado.

Que en la “II Reunión extraordinaria de la Comisión Nacional de Inmunización”, desarrollada el 1° de marzo de 2021, se instó a la elaboración de recomendaciones sobre el impacto de la vacunación en las licencias laborales y el potencial retorno a la actividad laboral de las personas vacunadas.

Que, de acuerdo con lo expresado en los fundamentos de la Resolución Conjunta del MINISTERIO DE SALUD y el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL Nº 4 del 8 de abril de 2021, según los resultados disponibles al momento las vacunas utilizadas en Argentina demostraron una adecuada eficacia para la prevención de las formas graves y de la muerte por la enfermedad, lo cual disminuye el riesgo y posibilita el retorno de las personas vacunadas a sus lugares de trabajo.

Que, con fecha 26 de marzo de 2021, el MINISTERIO DE SALUD comunicó, en virtud de lo acordado con todas las jurisdicciones en el marco del Consejo Federal de Salud (COFESA), nuevas recomendaciones relacionadas con la priorización de la primera dosis de las vacunas contra COVID-19 en la población objetivo, difiriendo la segunda dosis de cualquiera de las vacunas actualmente disponibles en nuestro país a un intervalo mínimo de DOCE (12) semanas desde la primera dosis.

Que dicha recomendación, que hace referencia a la extensión del intervalo mínimo sugerido entre ambas dosis y no a la suspensión de la segunda dosis, tiene como fin proteger lo antes posible a la mayor cantidad de personas con alguna condición de riesgo y reducir el impacto de las muertes por esta enfermedad.

Que todo lo anterior permite el establecimiento de pautas para el retorno a la actividad laboral presencial en contexto de pandemia de las personas trabajadoras vacunadas, con la debida observancia de las recomendaciones sanitarias en materia de prevención y control de la salud pública, sin poner en peligro los esquemas implementados para evitar la propagación del nuevo coronavirus SARS-CoV-2, virus responsable del COVID-19.

Que mediante la citada Resolución Conjunta Nº 4/21, se dispuso para el Sector Privado que los empleadores y las empleadoras podrán convocar al retorno a la actividad laboral presencial a las personas trabajadoras, incluidas las dispensadas por encontrarse comprendidas en los incisos a), b) y c) del artículo 1° de la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 207 del 16 de marzo de 2020 y sus modificatorias, que hubieren recibido al menos la primera dosis de cualquiera de las vacunas destinadas a generar inmunidad adquirida contra el COVID-19 autorizadas para su uso en la República Argentina, independientemente de la edad y la condición de riesgo, transcurridos CATORCE (14) días desde la inoculación.

Que la mencionada Resolución Conjunta fijó el criterio de adquisición de inmunidad, a los fines de la convocatoria de asistencia a los lugares de trabajo.

Que actualmente, la reducción de casos de COVID-19 positivos ha reducido la emergencia del sistema sanitario, por lo que resulta oportuno y conveniente la aplicación del criterio de convocatoria a los lugares de trabajo en el Sector Público Nacional.

Que la DIRECCIÓN NACIONAL de la OFICINA NACIONAL DE EMPLEO PÚBLICO de la SUBSECRETARÍA DE EMPLEO PÚBLICO de la SECRETARÍA DE GESTIÓN Y EMPLEO PÚBLICO de la JEFATURA DE GABINETE DE MINISTROS, se ha expedido en el ámbito de su competencia

Que mediante IF-2021-56983345-APN-DGAJ#JGM la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARÍA LEGAL de la SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, ha tomado la intervención de su competencia

Que la presente medida se dicta en uso de las facultades previstas por el artículo 2° del Anexo I del Decreto N° 1421 del 8 de agosto de 2002 y sus modificatorios, y por el Decreto N° 50 del 19 de diciembre de 2019 y sus modificatorios.

Por ello,

LA SECRETARIA DE GESTIÓN Y EMPLEO PÚBLICO DE LA JEFATURA DE GABINETE DE MINISTROS

RESUELVE:

ARTÍCULO 1º.- Establécese que las y los titulares de cada jurisdicción, organismo o entidad comprendido en el artículo 8° de la Ley N° 24.156 y sus modificatorios, podrán convocar al retorno a la actividad laboral presencial a las y los trabajadores que hubieren recibido al menos la primera dosis de cualquiera de las vacunas destinadas a generar inmunidad adquirida contra el COVID-19 autorizadas para su uso en la REPÚBLICA ARGENTINA, independientemente de la edad y la condición de riesgo, transcurridos CATORCE (14) días de la inoculación.

ARTÍCULO 2°.- Las personas trabajadoras de la salud con alto riesgo de exposición que se encuentren comprendidas en los incisos 2) y 3) del artículo 1° de la Decisión Administrativa Nº 390 del 16 de marzo de 2020 y su modificatoria, podrán ser convocadas una vez transcurridos CATORCE (14) días de haber completado el esquema de vacunación en su totalidad, independientemente de la edad y la condición de riesgo, sin perjuicio de lo

establecido en el artículo 5° de la presente.

ARTÍCULO 3º.- Las personas convocadas deberán presentar constancia fehaciente de vacunación correspondiente o manifestar, con carácter de declaración jurada, los motivos por los cuales no pudieron acceder a la vacunación.

ARTÍCULO 4º.- Las personas comprendidas en el ámbito alcanzado por la medida dispuesta en los artículos 1º y 2º de la presente resolución que tengan la posibilidad de acceder a la vacunación y opten por no vacunarse, deberán actuar de buena fe y llevar a cabo todo lo que esté a su alcance para evitar los perjuicios que su decisión pudiere ocasionar al normal desempeño de las organizaciones en las cuales prestan servicios.

ARTÍCULO 5°.- Exceptúase a las personas incluidas en el artículo 3°, incisos V y VI de la Resolución del MINISTERIO DE SALUD N° 627 del 19 de marzo de 2020 y su modificatoria, de lo previsto por los artículos 1° y 2º de la presente resolución.

ARTÍCULO 6°.- La presente medida comenzará a regir a partir del día de su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA.

ARTÍCULO 7°.- Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Ana Gabriela Castellani

e. 28/06/2021 N° 44514/21 v. 28/06/2021

Fecha de publicación 28/06/2021

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE INNOVACIÓN PÚBLICA

Resolución 65/2021

RESOL-2021-65-APN-SIP#JGM

Ciudad de Buenos Aires, 24/06/2021

VISTO el Expediente Electrónico N.° EX-2021-54431188-APN-SSGAIP#JGM, la Ley N.° 23.396, el Decreto N.° 945 de fecha 17 de noviembre de 2017, el Decreto N.° 50 de fecha 19 de diciembre de 2019 y sus modificatorios, el Decreto N.° 86 de fecha 27 de diciembre de 2019, el Documento del Proyecto PNUD ARG/20/008, y

CONSIDERANDO:

Que por el Expediente citado en el Visto, tramita un proyecto de Resolución tendiente a crear el Programa “Becas País Digital”.

Que mediante la Ley N.º 23.396, se aprobó el Acuerdo entre la República Argentina y el Programa de las Naciones Unidas para el Desarrollo (PNUD) firmado en Buenos Aires el 26 de febrero de 1985, en el cual se enuncian las condiciones básicas en las cuales el PNUD y sus Organismos de Ejecución prestarán asistencia al gobierno para llevar a cabo sus proyectos de desarrollo.

Que en el marco de la Ley precitada, se suscribió el Documento de Proyecto (PRODOC) del Proyecto PNUD ARG/20/008, denominado “Promoción de la inclusión digital y la igualdad a través de la Innovación Pública Federal”, en cuya Actividad N.° 3, “Apoyar la innovación de la gestión y administración pública eficaz para un gobierno abierto y digital inclusivo”, se estableció como objetivo la contratación de servicios de Universidades dedicadas a la formación de personas en habilidades digitales para llevar a cabo actividades de capacitación, dirigidas a personas mayores de 18 años con estudios de nivel secundario finalizados y que no se encuentren en el momento siendo beneficiarios de otra beca educativa otorgada por el Estado.

Que a través del Decreto N° 50/19, se aprobó el Organigrama de Aplicación de la Administración Nacional centralizada hasta nivel de Subsecretaría, creándose, entre otras, la SECRETARÍA DE INNOVACIÓN PÚBLICA dependiente de la JEFATURA DE GABINETE DE MINISTROS, entre cuyos objetivos se encuentra el de “Entender en la promoción del acceso universal a las nuevas tecnologías como herramientas de información y conocimiento (…)”.

Que con fecha 17 de noviembre de 2017, mediante el Decreto N° 945, se estableció que las “Jurisdicciones y Entidades de la Administración Pública Nacional comprendidas en el artículo 8° inciso a) de la Ley Nº 24.156 que ejecuten programas y proyectos con financiamiento externo multilateral, bilateral o regional y/o proyectos de participación público-privada a través de las unidades ejecutoras creadas a tal efecto, centralizarán la gestión y ejecución operativa, administrativa, presupuestaria y financiera-contable, comprendiendo las cuestiones fiduciarias y legales, sobre cumplimiento de las cuestiones ambientales y sociales, los procedimientos de contrataciones, como así también, la planificación, programación, monitoreo y auditoría de dichos programas y proyectos, a través de sus respectivas Subsecretarías de Coordinación Administrativa o áreas equivalentes, según corresponda.”.

Que, asimismo, mediante el artículo 2° de dicho Decreto, se estipuló que “Las funciones de coordinación y ejecución técnica de los programas y proyectos con financiamiento externo multilateral, bilateral o regional y/o proyectos de participación público-privada, actualmente desarrolladas por las unidades ejecutoras técnicas o por las áreas técnicas de unidades ejecutoras de programas, serán llevadas a cabo por las Secretarías y Subsecretarías o áreas equivalentes de carácter sustantivo de las Jurisdicciones y Entidades comprendidas por el artículo 8° inciso a) de la Ley Nº 24.156 con responsabilidad primaria en la materia de que se trate.”.

Que, en sentido concordante, por el ya citado Decreto N° 50/19, se estableció, entre los objetivos a cargo de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA, dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA, el de “Entender en la ejecución operativa y en los procesos de gestión administrativa, presupuestaria y financiera-contable de programas, proyectos, cooperaciones técnicas, donaciones y asistencias técnicas con financiamiento externo, como así también en los proyectos de participación público-privada, en coordinación con las áreas pertinentes de la SECRETARÍA DE COORDINACIÓN ADMINISTRATIVA.”.

Que, por su parte, entre los objetivos a cargo de la SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, establecidos en la precitada norma, se encuentra el de “Promover la creación de una red de innovación pública y gobierno abierto a nivel nacional generando espacios de trabajo colaborativo, intercambio y capacitación con el Sector Público Nacional, Provincial, de la Ciudad Autónoma de Buenos Aires y Municipal, el sector privado, académico y organizaciones de la sociedad civil” y el de “Asistir a la Secretaría en la promoción de políticas, programas y acuerdos de innovación pública en el territorio nacional, en particular en las Jurisdicciones provinciales, municipales y en la CIUDAD AUTÓNOMA DE BUENOS AIRES.”.

Que la creación del Programa “Becas País Digital” se funda en la necesidad de fomentar la inclusión digital y la participación de mujeres y diversidades en la industria de las Tecnologías de la Información y las Comunicaciones (TIC), constituyendo, asimismo, una acción de capacitación que promueva una formación integral que incluya conocimientos de programación, marketing digital y ciencia de datos, todo lo cual coadyuvará a dar respuesta a la demanda laboral de personas calificadas en habilidades digitales.

Que, atento lo hasta aquí expuesto, a fin de dar cumplimiento al objetivo señalado en el párrafo cuarto de la presente, resulta necesario crear el Programa “Becas País Digital”.

Que, asimismo, atento razones de eficiencia, resulta conveniente delegar su planificación, programación, gestión y ejecución en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la

SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, ambas dependientes de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que, al mismo tenor, resulta pertinente facultarlos para dictar las medidas complementarias a la presente y para suscribir convenios específicos y/o acuerdos con cámaras empresariales o entidades pertinentes a fin de cumplimentar los objetivos del Programa.

Que el gasto que demande la presente se atenderá con cargo a las partidas específicas del PROYECTO PNUD ARG/20/008 y del SAF 366 Jurisdicción 25 de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que la DIRECCIÓN DE ASUNTOS LEGALES DE INNOVACIÓN PÚBLICA, dependiente de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA de la SECRETARÍA DE INNOVACIÓN PÚBLICA, ha tomado la intervención de su competencia.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el Decreto N° 50/19 y por el Decreto N° 86/19.

Por ello,

LA SECRETARIA DE INNOVACIÓN PÚBLICA

RESUELVE:

ARTÍCULO 1°.- Créase el Programa “BECAS PAÍS DIGITAL” con el objeto de fomentar la inclusión digital y la participación de mujeres y diversidades en la industria de las Tecnologías de la Información y las Comunicaciones (TIC) y de capacitar en programación, marketing digital y ciencia de datos, a fin de responder a la demanda laboral de personas calificadas en habilidades digitales.

ARTÍCULO 2°.- Delégase la planificación, programación, gestión y ejecución del Programa creado en el artículo primero en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la SUBSECRETARÍA DE GOBIERNO ABIERTO Y PAÍS DIGITAL, ambas dependientes de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, quedando facultadas – en forma conjunta – para dictar las medidas complementarias a la presente y para suscribir convenios específicos y/o acuerdos específicos con cámaras empresariales o entidades pertinentes a fin de cumplimentar los objetivos de aquel.

ARTÍCULO 3°.- Delégase en la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA y en la SUBSECRETARIA DE GOBIERNO ABIERTO Y PAÍS DIGITAL la facultad, en forma conjunta, de aprobar las definiciones y el reglamento de bases y condiciones para la convocatoria “BECAS PAÍS DIGITAL”.

ARTÍCULO 4°.- El gasto que demande la presente medida sera atendido con cargo a las partidas específicas del PROYECTO PNUD ARG/20/008 y del SAF 366 Jurisdicción 25 de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

ARTÍCULO 5°.- Comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y archívese.

Micaela Sánchez Malcolm

e. 28/06/2021 N° 44104/21 v. 28/06/2021

Fecha de publicación 28/06/2021

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Informe

Número: IF-2021-53649652-APN-SSCPU#JGM

CIUDAD DE BUENOS AIRES
Martes 15 de Junio de 2021

Referencia: PROGRAMA SUMAR CAPACITACIÓN

Anexo I

PROGRAMA "SUMAR CAPACITACIÓN"

I. Fundamentación

A partir de las Misiones y Funciones de la SECRETARIA DE MEDIOS Y COMUNICACIÓN PÚBLICA vinculadas a fortalecer la libertad de expresión e impulsar la pluralidad cultural e informativa, se busca establecer el presente programa que consiste en la puesta en funcionamiento de un dispositivo de capacitación en pos de generar una estrategia de formación continua destinada a los actores de comunicación participantes de Medios de Gestión Social de todo el país.

En ese marco se pretende fomentar el empoderamiento de los medios de gestión social mediante el aporte de nuevos conocimientos y el perfeccionamiento de sus capacidades actuales tanto para la generación de contenidos de mayor calidad como así también para su vinculación con el público en general.

Así es posible desarrollar distintas iniciativas de formación integral en materia de comunicación destinada a impulsar herramientas que permitan involucrarse activamente a todos aquellos actores que desean participar como productores de la circulación informativa y de sentido en la sociedad.

En ese sentido, este Programa promueve la articulación e implementación de cursos de capacitación en conjunto

con asociaciones civiles sin fines de lucro, organizaciones sindicales, universidades nacionales, instituciones educativas terciarias y gobiernos locales entre otros actores; entendiendo que la comunicación actual demanda acciones permanentes del Estado orientadas a la profesionalización y reflexión crítica sobre el funcionamiento de los medios de comunicación.

II. Objetivos:

Objetivos generales:

. Promover articulaciones del Estado con los medios de gestión social de todas las regiones del país.

. Promover la formación como proceso permanente y necesario con miras al fortalecimiento de la pluralidad informativa

. Promover el fortalecimiento vincular con las organizaciones asociadas a la comunicación.

. Promover miradas y análisis críticos vinculadas al desarrollo de la comunicación

. Contribuir a la apropiación de herramientas conceptuales y políticas como parte del proceso de reconocimiento de la comunicación comunitaria.

. Garantizar el cuestionamiento a los modelos imperantes que reproducen los medios de comunicación masivos.

III. Finalidad

Apuntamos que al finalizar el proceso de formación lxs participantes se encuentren fortalecidxs para el ejercicio cotidiano de su desarrollo en el ámbito de la comunicación.

IV. Destinatarixs

Todas aquellas personas vinculadas de manera directa con los medios de gestión social, en cualquiera de sus formatos.

Asimismo, se invita a asociaciones civiles sin fines de lucro, organizaciones sindicales, universidades nacionales, instituciones educativas terciarias y gobiernos locales para la proyección de las distintas actividades curriculares.

V. Articulaciones institucionales

Consideramos indispensable abonar al intercambio con aquellas organizaciones con conocimiento en comunicación comunitaria, trayectoria en trabajo en ese campo, y acompañamientos de los medios en los diversos territorios.

El Programa conformará un equipo para dar respuesta a las necesidades del territorio que puedan ser abordadas desde la formación, garantizando la sinergia entre la Subsecretaría de contenidos públicos y las actorxs de la comunicación comunitaria.

A su vez, será responsabilidad de este equipo garantizar la evaluación continua y de proceso en la preparación y ejecución de los proyectos, garantizando un monitoreo de resultados que permitan asegurar el cumplimiento de los objetivos y, al mismo tiempo, mejorar el accionar del Programa.

VI. Modalidad de Trabajo

El programa consiste en la generación y puesta en funcionamiento de cursos de capacitación por parte de las asociaciones civiles con las cuales se suscribirán convenios específicos a tal efecto.

Los cursos contemplan una duración total de cuarenta y ocho (48) horas a desarrollarse en un plazo de dos meses. El tutor a cargo de los mismos deberá brindar seis (6) horas semanales, divididas en dos (2) horas de presentación y explicación de los contenidos de la clase de manera virtual; dos (2) horas de tareas de seguimiento de las actividades en la plataforma; dos (2) horas de trabajo en conjunto de los contenidos trabajados en la semana y el debate correspondiente a partir de las lecturas.

Es tarea de la parte conveniada determinar en primer término un referente del proyecto; presentar los contenidos de acuerdo a los lineamientos y objetivos del Programa; dictar la totalidad de horas de clases proyectadas; deberá contar con un equipo que garantice la articulación de la propuesta pedagógica, el seguimiento administrativo y la rendición de cuentas.

La Subsecretaría de contenidos públicos tiene a su cargo la coordinación general del Programa, su implementación y monitoreo.

Para garantizar los objetivos propuestos se priorizará y trabajará para la federalización del Programa, tanto en lo

comunicacional, en la selección de proyectos, como así también en su acompañamiento y adecuación que aseguren la posibilidad de acceder al mismo teniendo en cuenta las particularidades de lxs destinatarixs.

VII. Ejes generales para los cursos a desarrollarse en el periodo 2021/22

- Radio para adultos mayores.
- Radio I
- Radio II
- Realización de podcast
- Radioteatro
- Taller de locución
- Edición de sonido
- Nuevas Tecnologías en radio
- Producción periodística y Creatividad en radio
- Producción informativa
- Edición Artística
- Operación Técnica en Radio
- Marketing Digital
- Producción de videos en dispositivos móviles
- Taller de periodismo multimedia
- Cobertura inclusiva: perspectiva de género en las salas de redacción | discapacidad
- Community Manager
- Taller de fotoperiodismo móvil
- Utilización de herramientas Google | Analytics Google ads

- Comunicación efectiva
- Curso de oratoria
- Cybersegurdiad
- Aspectos legales para la creación de un medio de comunicación I
- Aspectos legales para la creación de un medio de comunicación II
- Registro de marca
- Plataformas Digitales
- Geomarketing
- Diseño web
- Introducción a software libre
- Social Media manager | Redes sociales como medio de comunicación
- Comercialización

VIII. Financiamiento

La Secretaría de medios y comunicación pública otorgará a la entidad conveniada la suma de pesos ciento cincuenta y ocho mil cuatrocientos ($158.400) por cada curso dictado conforme los lineamientos establecidos en el programa. La suma establecida surge de los siguientes parámetros

- Pesos setenta y dos mil ($72.000). - equivalente al sueldo del tutor, a un valor de $1.500.- la hora, conforme a seis (6) horas semanales por dos (2) meses;
- Pesos setenta y dos mil ($72.000) con motivo de la producción del curso;
- 10% sobre el total (Curso + sueldo) para tareas administrativas.

Para el año 2021 se prevé la generación de un total de veinticinco cursos de SUMAR CAPACITACIÓN por lo cual se requerirá a tal fin de un presupuesto de PESOS TRES MILLONES NOVECIENTOS SESENTA MIL

($3.960.000,00).

IX. Requisitos para la presentación de propuestas

La Subsecretaría de contenidos públicos tendrá a su cargo el establecimiento de los requisitos que deberán ser cumplidos por las entidades y organizaciones sociales que soliciten la producción y dictado de cursos en el marco del presente programa.

X. Rendición de cuentas e incumplimientos.

La Subsecretaría de contenidos públicos será la encargada de la implementación y control del mecanismo de rendición respecto al curso o cursos conveniados. Asimismo en caso de verificarse un incumplimiento total o parcial del proyecto conveniado en ningún caso se concretará la transferencia aludida en el punto VIII, o en su caso podrá exigirse la devolución parcial o total de la misma según corresponda.

Digitally signed by Gestion Documental Electronica
Date: 2021.06.15 14:07:59 -03:00

Jorge MENESES
Subsecretario
Subsecretaría de Contenidos Públicos
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2021.06.15 14:08:00 -03:00

JEFATURA DE GABINETE DE MINISTROS

SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA

Resolución 9618/2021

RESOL-2021-9618-APN-SMYCP#JGM

Ciudad de Buenos Aires, 24/06/2021

VISTO los EX-2021-53459015--APN-DRRHHMYCP#JGM y EX-2021-39865715- -APN-DRRHHMYCP#JGM, los Decretos N°. 50 del 19 de diciembre de 2019, el Decreto N° 40 del 8 de enero de 2020, sus modificatorios y complementarios, y

CONSIDERANDO:

Que entre los objetivos asignados por el Poder Ejecutivo Nacional en el Decreto 50/19 sus modificatorios y complementarios, esta SECRETARÍA DE MEDIOS Y COMUNICACIÓN PÚBLICA se encuentra el de "(…) Fortalecer la libertad de expresión y la pluralidad cultural e informativa; e intervenir en acciones de vinculación del ESTADO NACIONAL con la ciudadanía, en el ámbito de su competencia (…)".

Que, asimismo, la SUBSECRETARÍA DE CONTENIDOS PÚBLICOS tiene entre sus objetivos el de "(…) Participar en la administración y funcionamiento de la formulación y ejecución de políticas de inclusión digital, con criterio federal en el ámbito de su competencia; gestionando a su vez, políticas públicas de promoción de contenidos para actores locales (…)".

Que, en esa línea esta Secretaría, en el marco del EX-2021-39865715- -APN-DRRHHMYCP#JGM ha propiciado el desarrollo de la página web SINERGIA (https://sinergia.jgm.gob.ar/), buscando generar un punto de encuentro entre el ESTADO NACIONAL y los medios de comunicación audiovisual de gestión social de la República Argentina.

Que el portal posee un espacio de capacitación a los fines de brindar herramientas para todas aquellas personas que, vinculadas a los medios de gestión social, deseen participar como productores de sentido en la circulación informativa en la sociedad.

Que, asimismo, la capacitación constituye una herramienta clave no sólo para desarrollar y/o potenciar la innovación y la productividad, sino además que permite mejorar el desempeño en la gestión de los medios de comunicación, a través de la generación de nuevos conocimientos que se traduzcan en mejores prácticas que fortalezcan y pluralicen la libertad de expresión e informativa.

Que, asociado a ello, resulta oportuno destacar la relación existente entre las políticas en materia de capacitación, con el estudio y análisis de las necesidades concretas de los medios de gestión social, permitiendo para tales fines, la formulación de desarrollos que coadyuven a incoar de manera eficiente las acciones estatales con las demandas genuinas del sector.

Que, por tal motivo, resulta imperioso establecer un programa que consista en la puesta en funcionamiento de un dispositivo de capacitación en pos de generar una estrategia de formación continua destinada a los actores de comunicación participantes de Medios de Gestión Social de todo el país.

Que la DIRECCIÓN TECNICO ADMINISTRATIVA DE MEDIOS Y COMUNICACIÓN PÚBLICA ha tomado la intervención de su competencia.

Que la DIRECCIÓN DE ASUNTOS LEGALES DE MEDIOS Y COMUNICACIÓN PÚBLICA ha tomado la intervención de su competencia.

Que la presente medida se dicta de conformidad con las atribuciones y facultades otorgada por el Decreto Nº 50/2019 y sus modificatorios y el Decreto 40/2020.

Por ello,

EL SECRETARIO DE MEDIOS Y COMUNICACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS

RESUELVE:

ARTICULO 1°. – Créase el PROGRAMA “SUMAR CAPACITACIÓN” con el objetivo principal de fortalecer la libertad de expresión, generando una mayor pluralidad cultural e informativa mediante la formación de los actores vinculados a los medios de gestión social de la República Argentina.

ARTÍCULO 2°. – Apruébense los lineamientos generales y acciones del PROGRAMA “SUMAR CAPACITACIÓN” que se encuentran en el ANEXO I registrado bajo el número IF-2021-53649652-APN-SSCPU#JGM que forma parte integrante de la presente.

ARTÍCULO 3°. – La SUBSECRETARÍA DE CONTENIDOS PÚBLICOS tendrá a su cargo el desarrollo de los mecanismos y procedimientos necesarios para la implementación del PROGRAMA creado en el ARTÍCULO 1º de la presente resolución, con intervención de las áreas técnicas pertinentes dependientes de la SUBSECRETARÍA DE GESTIÓN OPERATIVA DE MEDIOS PÚBLICOS.

ARTICULO 4°. – El gasto que demande la presente medida se atenderá con cargo a la Partida 5.1.4 – Ayudas sociales a personas, de la Categoría Programática 75 - Acciones para la federalización de la comunicación pública y de los contenidos, de este SAF 347 – Secretaría de Medios y Comunicación Pública.

ARTÍCULO 5°. - La presente Resolución entrará en vigencia el día de su publicación en el Boletín Oficial.

ARTÍCULO 6°. – Comuníquese, publíquese, dése a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL. Cumplido, archívese.

Juan Francisco Meritello

NOTA: El/los Anexo/s que integra/n este(a) Resolución se publican en la edición web del BORA -www.boletinoficial.gob.ar-

e. 28/06/2021 N° 44298/21 v. 28/06/2021

Fecha de publicación 28/06/2021

Contacto

Dirección Servicios Legislativos

Avda. Rivadavia 1864, 3er piso , Of. 327

Palacio del Congreso CABA (CP 1033)

Teléfono: (005411) 4378-5626

servicioslegislativos@bcn.gob.ar

www.bcn.gob.ar