DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL

iniuRe

Instituto de la Juventud Regia

INSTITUTO DE LA JUVENTUD REGIA DEL MUNICIPIO DE MONTERREY

2024

CONTENIDO

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL INSTITUTO DE LA JUVENTUD REGIA DEL MUNICIPIO DE MONTERREY

INTRODUCCIÓN

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León se mencionan las bases, principios, procedimientos así como el tratamiento que garantiza la protección de los datos personales de los ciudadanos en posesión del Instituto de la Juventud Regia de la Administración Pública Municipal del Municipio de Monterrey Paramunicipal, como sujetos obligados, teniendo en base dicha normatividad, y en cumplimiento de lo establecido en el Artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se crea el presente documento de seguridad.

El presente documento de seguridad deberá contener por lo menos el inventario de datos personales; las funciones y obligaciones de las personas que tratan los datos personales; el análisis de riesgos; el análisis de brecha; el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad; y el programa general de capacitación.

En ese sentido, el Instituto de la Juventud Regia, a través de la Coordinación de Planeación en conjunto con el área de Proyectos Estratégicos y encargados de cada proyecto o servidor público generador de información, han realizado acciones y actividades que tuvieron como finalidad establecer principios para la creación de este documento.

Para recabar un diagnóstico específico se realizó un cuestionario a todo el personal que trata datos personales a través de los Titulares de las Unidades Administrativas de la Administración Pública Municipal del Municipio de Monterrey y sus Paramunicipales, con la finalidad de detectar medidas de seguridad con las que ya contaba cada área y dependencia, analizar las brechas de seguridad y definir posibles riesgos.

Una vez contestado el cuestionario, se analizó la información recabada, lo que permitió la creación de las medidas de seguridad. A partir de los inventarios iniciales de las bases de datos personales y diversas acciones, se generaron cada una de las partes que integran el presente documento de seguridad, siguiendo como objetivo el propiciar la protección de los datos personales de la forma más completa, ello encaminado a lograr el adecuado tratamiento de los datos personales.

MARCO NORMATIVO

Constitución Política de los Estados Unidos Mexicanos

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

Para efectos de lo dispuesto en el presente artículo se observará lo siguiente:

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán, a través de los medios electrónicos disponibles, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

El organismo autónomo previsto en esta fracción, se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros. También conocerá de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley.

El organismo garante federal, de oficio o a petición fundada del organismo garante equivalente de las entidades federativas, podrá conocer de los recursos de revisión que por su interés y trascendencia así lo ameriten.

La ley establecerá aquella información que se considere reservada o confidencial.

Las resoluciones del organismo garante son vinculatorias, definitivas e inatacables para los sujetos obligados. El Consejero Jurídico del Gobierno podrá interponer recurso de revisión ante la Suprema Corte de Justicia de la Nación en los términos que establezca la ley, sólo en el caso que dichas resoluciones puedan poner en peligro la seguridad nacional conforme a la ley de la materia.

El organismo garante se integra por siete comisionados. Para su nombramiento, la Cámara de Senadores, previa realización de una amplia consulta a la sociedad, a propuesta de los grupos parlamentarios, con el voto de las dos terceras partes de los miembros presentes, nombrará al comisionado que deba cubrir la vacante, siguiendo el proceso establecido en la ley. El nombramiento podrá ser objetado por el Presidente de

la República en un plazo de diez días hábiles. Si el Presidente de la República no objetara el nombramiento dentro de dicho plazo, ocupará el cargo de comisionado la persona nombrada por el Senado de la República.

En caso de que el Presidente de la República objetara el nombramiento, la Cámara de Senadores nombrará una nueva propuesta, en los términos del párrafo anterior, pero con una votación de las tres quintas partes de los miembros presentes. Si este segundo nombramiento fuera objetado, la Cámara de Senadores, en los términos del párrafo anterior, con la votación de las tres quintas partes de los miembros presentes, designará al comisionado que ocupará la vacante.

Los comisionados durarán en su encargo siete años y deberán cumplir con los requisitos previstos en las fracciones I, II, IV, V y VI del artículo 95 de esta Constitución, no podrán tener otro empleo, cargo o comisión, con excepción de los no remunerados en instituciones docentes, científicas o de beneficencia, sólo podrán ser removidos de su cargo en los términos del Título Cuarto de esta Constitución y serán sujetos de juicio político.

En la conformación del organismo garante se procurará la equidad de género.

El comisionado presidente será designado por los propios comisionados, mediante voto secreto, por un periodo de tres años, con posibilidad de ser reelecto por un periodo igual; estará obligado a rendir un informe anual ante el Senado, en la fecha y en los términos que disponga la ley.

El organismo garante tendrá un Consejo Consultivo, integrado por diez consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

La ley establecerá las medidas de apremio que podrá imponer el organismo garante para asegurar el cumplimiento de sus decisiones.

Toda autoridad y servidor público estará obligado a coadyuvar con el organismo garante y sus integrantes para el buen desempeño de sus funciones.

El organismo garante coordinará sus acciones con la Auditoría Superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de las entidades federativas, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano.

B. En materia de radiodifusión y telecomunicaciones:

I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.

II. Las telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias.

III. La radiodifusión es un servicio público de interés general, por lo que el Estado garantizará que sea prestado en condiciones de competencia y calidad y brinde los beneficios de la cultura a toda la población, preservando la pluralidad y la veracidad de la información, así como el fomento de los valores de la identidad nacional, contribuyendo a los fines establecidos en el artículo 3o. de esta Constitución.

IV. Se prohíbe la transmisión de publicidad o propaganda presentada como información periodística o noticiosa; se establecerán las condiciones que deben regir los contenidos y la contratación de los servicios para su transmisión al público, incluidas aquellas relativas a la responsabilidad de los concesionarios respecto de la información transmitida por cuenta de terceros, sin afectar la libertad de expresión y de difusión.

V. La ley establecerá un organismo público descentralizado con autonomía técnica, operativa, de decisión y de gestión, que tendrá por objeto proveer el servicio de radiodifusión sin fines de lucro, a efecto de asegurar el acceso al mayor número de personas en cada una de las entidades de la Federación, a contenidos que promuevan la integración nacional, la formación educativa, cultural y cívica, la igualdad entre mujeres y hombres, la difusión de información imparcial, objetiva, oportuna y veraz del acontecer nacional e internacional, y dar espacio a las obras de producción independiente, así como a la expresión de la diversidad y pluralidad de ideas y opiniones que fortalezcan la vida democrática de la sociedad.

El organismo público contará con un Consejo Ciudadano con el objeto de asegurar su independencia y una política editorial imparcial y objetiva. Será integrado por nueve consejeros honorarios que serán elegidos mediante una amplia consulta pública por el voto de dos terceras partes de los miembros presentes de la Cámara de Senadores o, en sus recesos, de la Comisión Permanente. Los consejeros desempeñarán su encargo en forma escalonada, por lo que anualmente serán sustituidos los dos de mayor antigüedad en el cargo, salvo que fuesen ratificados por el Senado para un segundo periodo.

El Presidente del organismo público será designado, a propuesta del Ejecutivo Federal, con el voto de dos terceras partes de los miembros presentes de la Cámara de Senadores o, en sus recesos, de la Comisión Permanente; durará en su encargo cinco años, podrá ser designado para un nuevo periodo por una sola vez, y sólo podrá ser removido por el Senado mediante la misma mayoría.

El Presidente del organismo presentará anualmente a los Poderes Ejecutivo y Legislativo de la Unión un informe de actividades; al efecto comparecerá ante las Cámaras del Congreso en los términos que dispongan las leyes.

VI. La ley establecerá los derechos de los usuarios de telecomunicaciones, de las audiencias, así como los mecanismos para su protección.

Artículo 13.- Las personas tienen derecho a la protección a la vida privada, incluyendo la información personal que se encuentre en las tecnologías de la información y comunicación. Los sujetos obligados, en términos de la legislación general aplicable, deberán proteger los datos personales en posesión de las autoridades.

El Estado promoverá la protección y desarrollo de los derechos y las libertades reconocidos en esta Constitución dentro del ámbito digital y serán plenamente aplicables en ese ámbito. Se promoverá, a través de políticas públicas, la inclusión de todas las personas de la entidad para el ejercicio de sus derechos de forma digital, de manera que se procure el bien común y el fortalecimiento de la comunidad.

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.

Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a disposición de la autoridad civil más cercana y ésta con la misma prontitud, a la del Ministerio Público. Existirá un registro inmediato de la detención.

Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o

circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder.

En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley.

La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días.

Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.

Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.

En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia.

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los

derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces, Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.

La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.

La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley.

En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.

Constitución Política del Estado Libre y Soberano de Nuevo León

Artículo 162.- Toda la información en posesión de cualquier autoridad, dependencia, unidades administrativas, entidad, órgano u organismo municipal o de los Poderes Ejecutivo, Legislativo, Judicial o del ámbito municipal, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal y municipal, es pública, y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las Leyes. Para la interpretación de este derecho, prevalecerá el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuáles procederá la declaración de inexistencia de la información.

Se establecerán mecanismos de acceso a la información y procedimientos de inconformidad expeditos que se sustanciarán ante el organismo autónomo especializado e imparcial que establece esta Constitución, de acuerdo a las siguientes bases mínimas:

I. La información relativa a la vida privada y datos personales será protegida en los términos y con las excepciones que determine la ley.
II. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos, en los términos que determine la legislación aplicable.
III. Un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, conformado por ciudadanos designados por el Poder Legislativo, con plena autonomía técnica, de gestión, de capacidad para decidir sobre el ejercicio

de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

El organismo autónomo previsto en esta fracción, se denominará Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley que emita el Congreso del Estado para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, dependencia, unidades administrativas, entidad, órgano u organismo municipal o que forme parte de alguno de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito estatal o municipal.

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales podrá remitir los procedimientos de inconformidad que por su interés y trascendencia así lo ameriten al organismo garante federal, para que conozca de los mismos.

La ley establecerá aquella información que se considere reservada o confidencial.

Las resoluciones del Instituto Estatal Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales son vinculatorias, definitivas e inatacables para los sujetos obligados.

En la conformación del Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales se debe respetar la paridad de género, y será integrado por cinco consejeros, quienes deberán reunir los siguientes requisitos:

a) Ser ciudadano mexicano, en pleno ejercicio de sus derechos políticos, e inscrito en la lista nominal de electores del Estado.
b) Tener treinta años de edad cumplidos cuando menos al día de la propuesta de su designación.
c) Ser profesionista, con experiencia mínima de cinco años a la fecha de la propuesta de su designación, con conocimientos y experiencia afines en materia de acceso a la información pública y protección de datos personales.
d) Tener reputación de independencia y buen juicio, y haberse desempeñado destacadamente en actividades profesionales, de servicio público o académicas.
e) No haber sido condenado por delito doloso.

f) No haber desempeñado en el período de dos años anteriores a la fecha de la propuesta de su designación ningún cargo público en la federación, las entidades federativas o los municipios.
g) No haber sido dirigente de ningún partido o asociación política a nivel nacional, estatal o municipal en el período de cinco años anteriores a la fecha de la propuesta para su designación.
h) No haber sido postulado como candidato para algún cargo de elección popular en el período de tres años anteriores a la fecha de la propuesta de su designación.

Los consejeros, previa convocatoria pública, serán designados por el Congreso del Estado en sesión pública, mediante el voto de las dos terceras partes de sus integrantes. De no alcanzarse dicha votación, se procederá a la designación mediante insaculación.

Los consejeros durarán en el cargo un período de siete años. Solo podrán ser removidos del cargo en los términos de lo dispuesto en el Título VII de esta Constitución y en la Ley de Responsabilidades Administrativas del Estado Nuevo León.

El presidente será designado por los mismos consejeros, mediante voto secreto. Su cargo será por un período de dos años, con posibilidad de ser reelecto por un periodo igual. El consejero presidente estará obligado a rendir un informe anual ante el Congreso del Estado, en los términos que disponga la ley.

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales tendrá un Consejo Consultivo, integrado por diez consejeros de carácter honorífico que serán elegidos por el voto de las dos terceras partes de los integrantes del Congreso del Estado. La ley determinará los procedimientos a seguir para la presentación de las propuestas por el propio Congreso. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

La ley establecerá las medidas de apremio que podrá imponer el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales para asegurar el cumplimiento de sus decisiones.

Toda autoridad y servidor público estará obligada a coadyuvar con el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales y sus integrantes para el buen desempeño de sus funciones.

El Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales coordinará sus acciones con la entidad de fiscalización superior del Estado, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, con el objeto de fortalecer la rendición de cuentas del Estado mexicano.

IV. Garantizar que la ciudadanía disponga de los datos abiertos en materia de contrataciones públicas a fin de promover el acceso a la información pública y generar conocimiento con la finalidad de gestionar sistemas electrónicos que formulen herramientas y metodologías reutilizables para visualizar los datos de contrataciones,

proporcionar inteligencia empresarial, crear circuitos de retroalimentación entre el gobierno, las empresas y los ciudadanos y detectar hechos de corrupción mediante la vinculación de datos sobre contrataciones beneficiarios finales y funcionarios públicos, y a su vez facilitar una vigilancia ciudadana a través de la publicación y difusión de la información que se derive de los procedimientos de contrataciones.

V. Se establecerán mecanismos eficientes, de universal y fácil acceso, para que los sujetos obligados publiquen a través de los medios electrónicos disponibles la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos; así como la cultura de la transparencia y el acceso a la información.

VI. La inobservancia a las disposiciones en materia de transparencia y acceso a la información será sancionada en los términos que disponga la ley

Ley de Protección de Datos Personales en Popsesión de Sujetos Obligados del Estado de Nuevo León:

Artículo 3. Para los efectos de la presente Ley se entenderá por: (...)

XV. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Artículo 41. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad; y

VII. El programa general de capacitación.

Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León:

Artículo 54. Con relación a lo previsto en el numeral 38, fracción 111, de la Ley, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;

II. Las finalidades de cada tratamiento de datos personales;

III. El catálogo de formato de almacenamiento, así como la descripción general de ubicación física y/o electrónica de los datos personales;

IV. El catálogo de formato de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Artículo 56. Para dar cumplimiento al artículo 38, fracción IV, de la Ley, el responsable deberá realizar un análisis de riesgos de los datos personales tratados, considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;

III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;

IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y;

V. Los factores previstos en el artículo 37 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Artículo 57. Con relación al artículo 38, fracción V, de la Ley, para la realización del análisis de brecha, el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;

II. Las medidas de seguridad faltantes; y

III. La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

Artículo 58. De conformidad con lo dispuesto en el artículo 38, fracción VI, de la Ley, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de

acuerdo con el resultado del análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos asignados; el personal interno y externo en su organización y las fechas de compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Artículo 59. Con relación al artículo 38, fracción VII, de la Ley, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explot§das por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Artículo 60. Para el cumplimiento de lo previsto en el artículo 38, fracción VIII, de la Ley, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tenga por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones de sistemas de gestión;

II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

III. Las consecuencias de incumplimiento de los requerimientos legales o requisitos organizacionales, y;

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

GLOSARIO

Activo: Es la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para el responsable.

Anonimización: Es el reducir al mínimo los riesgos de reidentificación de los datos, manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personales, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización, no conlleva una distorsión de los datos reales.

Bases de Datos: Es el conjunto ordenado de datos personales referentes a una persona física identificada condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Confidencialidad: Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no automatizados.

Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León (INFONL): Es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, conformado por ciudadanos designados por el Poder Legislativo, con plena autonomía técnica, de gestión, de capacidad para decidir sobre el ejercicio de su derecho de acceso a la información pública y ala protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

Derechos Arco: Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Disociación: Es el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, debido a su estructura, el contenido o grado de desagregación, la identificación del mismo.

Disponibilidad: Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable

para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

DT: Dirección de Transparencia de la Contraloría Municipal de Monterrey.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.

Evaluación del impacto en la protección de datos personales: Es el documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.

Hardware: Es el conjunto de componentes físicos de los que ésta hecho el equipo.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI): Es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el acceso a la información pública y el de protección de datos personales.

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos.

Inventario de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de la Administración Pública Municipal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

Lineamientos: Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León.

Medidas de Seguridad: Es el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de Seguridad Administrativas: Son la Políticas y Procedimientos para la gestión, soport y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.

Medidas de Seguridad Físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medias de Seguridad Técnicas: Son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

N/A: No aplica.

Red de área local (LAN): Es una red de computadoras que abarca un área reducida a una casa, departamento o edificio.

Respaldo: Es una copia de la información que se genera, utiliza y actualiza a lo largo del tiempo; también este término se emplea para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, software de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

Responsable: Lo es el Municipio de Monterrey, al ser quien determina los fines, medios, alcance y demás cuestiones relacionadas con el tratamiento de los datos personales.

Riesgo: Es la combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad: Es la probabilidad de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio del Municipio de Monterrey.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Supresión: Es la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad establecidas por el responsable.

Titular: Es la persona física a quien pertenecen los datos personales.

Transferencia: Es toda comunicación de datos personales fuera del Sujeto Obligado

Tratamiento: Es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionado esto con la obtención, uso. registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Software: Es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

Unidad administrativa: Aquella(s) que se encuentra(n) subordinada(s) jerárquica y funcionalmente a las Dependencias señaladas en el artículo 16 del Reglamento de la Administración Pública Municipal de Monterrey, Nuevo León, o a las Entidades de la Administración Pública Paramunicipal; integrada por recursos humanos, materiales, financieros y demás archivos físicos y electrónicos, dentro de la administración pública Municipal.

I.- INVENTARIO DE DATOS PERSONALES

Se entiende por "inventario de datos personales" al control de documentos y tratamiento de datos personales que realizan la unidad administrativa del Instituto de la Juventud Regia de la Administración Pública Municipal del Municipio de Monterrey Paramunicipal que se encuentran almacenados tanto física como electrónicamente.

Dichos tratamientos de datos personales, se presentan por tratamiento de datos personales previstas en base a los Avisos de Privacidad dados de alta en la página oficial del Municipio de Monterrey y de los programas vigente del Instituto de la Juventud Regia así como el Reglamento Orgánico del Instituto de la Juventud Regia y normativa aplicable.

Lo anterior, tiene sustento en los artículos 38 fracción III y 41 fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, pues disponen la obligación de los responsables que cuenten con el inventario de datos personales y que este sea parte de las medidas de seguridad implementadas y del documento respectivo, lo anterior con el fin de tener en cuenta el volumen de datos que se tratan al interior de la organización responsable.

Descripción y estructura de las bases de datos de tratamiento de datos personales

En la descripción de cada base de tratamiento, se indica cuales son los datos que se recaban, la finalidad con la que se obtienen, forma de obtención, así como el fundamento legal que faculta al área administrativa para el tratamiento de dichos datos personales, los medios de almacenamiento, sitios de resguardo, si existe un encargado que actúe a cuenta y nombre de la Unidad Administrativa y la persona servidora pública encargada de administrar las bases o inventario de datos personales así como subordinados que tienen acceso a las mismas.

Es importante mencionar que los inventarios de datos personales se define la "categoría de los datos personales", estableciendo los tipos de datos personales que pueden estar sujetos a tratamiento de acuerdo a las atribuciones de cada unidad administrativa:

- Datos de identificación y contacto: Nombre, género, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales, identificación personal, imagen.

- Datos sobre características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, cicatrices, tatuajes.

- Datos biométricos: Huella Dactilar.

- Datos laborales: Puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/ capacitación laboral.

- Datos académicos: Trayectoria educativa, escolaridad, título, cédula profesional, certificados y reconocimientos

- Datos patrimoniales y/o financieros: Bienes muebles, bienes inmuebles, ingresos, egresos y cuentas bancarias, información fiscal, historial crediticio, número de tarjeta, seguros, afores.

- Datos legales: Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros).

- Datos relativos a la salud: Estado de salud físico presente, pasado o futuro; diagnóstico, estado de salud mental, información genérica.

- Datos personales de naturaleza pública: Datos que por mandato legal son de acceso público.

- Datos sobre pasatiempos, entretenimiento y diversión: Pasatiempos, aficiones, deportes, juegos de interés.

En cuanto a la sección de "forma de obtención directa / indirectamente del titular medios físicos / electrónicos, de la referida tabla, a continuación, se describen el tipo de personas de quienes se obtienen y cómo se recaban datos personales que puedan estar sujetos a tratamiento de acuerdo a las atribuciones de cada unidad administrativa:

- Personas que laboran en el Instituto de la Juventud Regia de las distintas coordinaciones y áreas.

- Personas externas que participan en actividades que llevan a cabo las distintas coordinaciones y áreas del Instituto de la Juventud Regia así como dependencias de la administración central y paramunicipal (capacitaciones y cursos).

- Personas externas que prestan algún servicio al Instituto de la Juventud Regia y dependencias de la administración central y paramunicipal que participen en colaboración.

De igual manera se describen las finalidades de cada uno de los tratamientos, el fundamento legal que faculta cada área para tratar datos personales, los formatos en los que se encuentra la información, así como los medios de almacenamiento, por lo que, a fin de exponer primeramente los tratamientos que se llevan a cabo al interior del Instituto de la Juventud Regia se enlistan a continuación:

Catálogo de tratamiento de datos personales:

Instituto de la Juventud Regia	ACOMPAÑAMIENTO ACADÉMICO
Instituto de la Juventud Regia	ASESORÍAS UANL

Instituto de la Juventud Regia	BANQUETERAS
Instituto de la Juventud Regia	BECAS
Instituto de la Juventud Regia	BOOTCAMP DE EMPRENDIMIENTO
Instituto de la Juventud Regia	BRIGADAS INJURE
Instituto de la Juventud Regia	CAELE CON IDEAS
Instituto de la Juventud Regia	COLOR EN LAS CALLES
Instituto de la Juventud Regia	CONFERENCIAS POTENCIA JOVEN
Instituto de la Juventud Regia	CULTURA FÍSICA Y DEPORTE PREVENTIVO
Instituto de la Juventud Regia	CURSOS ICET
Instituto de la Juventud Regia	EMPRENDE A LO REGIO
Instituto de la Juventud Regia	ENTRE MANOS NOS HABLAMOS
Instituto de la Juventud Regia	INJURED
Instituto de la Juventud Regia	INJUREFEST
Instituto de la Juventud Regia	JALATE A MADRID
Instituto de la Juventud Regia	JUVENTUDES POR LA INNOVACIÓN
Instituto de la Juventud Regia	JUVENTUD(ES) MONTERREY
Instituto de la Juventud Regia	JUVENTUDES SANAS
Instituto de la Juventud Regia	NÚTRETE A LO REGIO
Instituto de la Juventud Regia	POTENCIA JÓVEN
Instituto de la Juventud Regia	PRIMER EMPLEO Y EMPRENDIMIENTO
Instituto de la Juventud Regia	PROYECTORES
Instituto de la Juventud Regia	REDES SOCIALES
Instituto de la Juventud Regia	REURBANIZARTE

Instituto de la Juventud Regia	TERAPIA DE A GRAPA
Instituto de la Juventud Regia	SISTEMA DE CÁMARAS DE SEGURIDAD
Instituto de la Juventud Regia	PROGRAMA DE TUTORÍAS ACADÉMICAS
Instituto de la Juventud Regia	ENCUESTA DE SATISFACCIÓN INJURE
Instituto de la Juventud Regia	ENSAMBLE CULTURAL
Instituto de la Juventud Regia	TORNEO RELÁMPAGO INJURE
Instituto de la Juventud Regia	RETO JUVENTUDES SANAS
Instituto de la Juventud Regia	CURSOS DE OFICIO INJURE
Instituto de la Juventud Regia	EVENTO VIERNES GAMER
Instituto de la Juventud Regia	JUVENTUDES A MONTERREY
Instituto de la Juventud Regia	BIBLIOTECA INJURE
Instituto de la Juventud Regia	CASA JUVENTUDES
Instituto de la Juventud Regia	CENTROS DE LA JUVENTUD
Instituto de la Juventud Regia	ACCESO JÓVEN
Instituto de la Juventud Regia	APOYOS DIVERSOS INJURE
Instituto de la Juventud Regia	PREPA INJURE
Instituto de la Juventud Regia	K.OMBATE TUS MIEDOS
Instituto de la Juventud Regia	LETRAS JÓVENES
Instituto de la Juventud Regia	CONSEJO CONSULTIVO CIUDADANO
Instituto de la Juventud Regia	INJUREMUN
Instituto de la Juventud Regia	EVENTO VIERNES GAMER

Liga electrónica donde se pueden consultar los inventarios de los datos personales cuyos tratamientos fueron descritos en las tablas previamente establecidas.

https://drive.google.com/drive/folders/1a0ApoU2IQyafreTsqeeKFMMLQIJJioot?usp=sharing

II.- LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Para la aplicación correcta de este documento, es necesario establecer los deberes de las personas servidoras públicas de las coordinaciones y áreas correspondientes del Instituto de la Juventud Regia que participan en el tratamiento de los datos personales derivado de sus atribuciones.

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
3. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
4. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
5. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.
6. Informar a la dirección de transparencia sobre los cambios que sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
7. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
8. Informar a la dirección de transparencia, en caso de detectar alguna vulneración de datos personales.

Son obligaciones de los Responsables de las Unidades de Transparencia en relación al tratamiento de los datos personales, las previstas en el artículo 99 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;

III. Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;

V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO; y

VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, previstas en el artículo 98 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por la Comisión;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales; y

VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales;

particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Reglamento Orgánico del Instituto de la Juventud Regia de la Ciudad de Monterrey

Artículo 3. El Instituto tiene por objeto lo siguiente:

I. Llevar a cabo programas, acciones, actividades y gestiones que favorezcan a los jóvenes sin discriminación alguna;
II. Implementar y operar programas para brindar atención a los jóvenes, en función de sus principales necesidades y problemáticas, a fin de proporcionar herramientas para fomentar su desarrollo integral;

Artículo 4. Para el cumplimiento de su objeto, el Instituto tendrá las siguientes atribuciones y obligaciones:

VI. Operar e implementar programas integrales que vayan dirigidos a disminuir la drogadicción, la inestabilidad emocional y la desintegración familiar, amén de campañas de orientación en salud reproductiva y educación sexual;
VII. Instalar y administrar centros municipales de atención a jóvenes, los cuales deberán de estar ubicados preferentemente en sectores populares, a fin de proporcionarles atención y orientación de manera directa e inmediata;
IX. Llevar a cabo en coordinación con las dependencias y entidades de la Administración Pública Federal, Estatal y Municipal, acciones destinadas a mejorar el nivel de vida de los jóvenes, así como sus expectativas familiares, sociales, culturales y derechos;
XI. Proporcionar información, y gestionar apoyos ante diversas instancias públicas y privadas, que permitan aplicar medidas en favor de la juventud;
XX. Desarrollar actividades que estimulen las habilidades artísticas, culturales y la expresión creativa de la juventud;
XXI. Analizar, y en su caso aprobar, los estímulos a jóvenes que demuestren tener facultades extraordinarias en la práctica de una disciplina artística, deportiva o científica;
XXIV. Gestionar ante las instituciones educativas públicas y privadas, el establecimiento de programas educativos, becas y apoyos financieros que alienten y estimulen la continuidad de los procesos de enseñanza y aprendizaje de los jóvenes;

III.- ANÁLISIS DE RIESGOS

El análisis de riesgo tiene como objetivo alinear la protección de los datos personales que se trate en el Municipio de Monterrey y por lo tanto en el Instituto de la Juventud Regia, con la evolución de las actividades que se realizan en el instituto, para anticiparse y prepararse para los nuevos retos que se suscitan día con día y en la complicidad de las actividades, lo recomendable es tener una responsabilidad proactiva ante el tratamiento de los datos personales gestionando los riesgos y el impacto que estos podrían generar.

En ese sentido, la gestión de riesgos consiste en implementar un conjunto de acciones definidas con el propósito de controlar la probabilidad de consecuencias o impactos que una actividad puede tener sobre los datos personales que posee el Instituto de la Juventud Regia,

los cuales han de ser protegidos, pues se pretende garantizar el servicio público que se otorga, por lo que debe de identificarse la naturaleza, el ámbito y fines de los tratamientos de datos personales, para poder detectar los niveles de posible vulnerabilidad de la información.

A fin de precisar la medición del nivel de impacto que pudieran tener las vulneraciones a la seguridad de los datos personales, se realiza la siguiente relación de nivel de impacto con descripción del impacto:

Nivel de impacto	Descripción del impacto al presentar vulneración a los tratamientos de datos personales
Muy significativo	• Afecta el ejercicio de los derechos fundamentales y libertades públicas establecidas en la constitución y sus consecuencias son irreversibles. • Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales y es irreversible. • Causa un daño social significativo como la discriminación y es irreversible. • Afecta interesados en situación de especial vulnerabilidad en particular niños y de forma irreversible. • Causa pérdidas morales o materiales significativas e irreversibles.
Significativo	• Los casos anteriores cuando los efectos son irreversibles. • Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos. • Se produce o puede producirse usurpación de la identidad de los interesados. • Pueden producirse pérdidas financieras significativas a los interesados y/o pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad. • Existe un perjuicio social para los interesados o determinados colectivos interesados.
Limitado	• Pérdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter irreversible. • Pérdidas financieras insignificantes e irreversibles y/o pérdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales.

Muy limitado	• En el caso anterior, cuando todos los efectos son reversibles.

Ahora bien, existen probabilidades de vulneraciones de acuerdo a la documentación generada en base a los tratamientos, o bien, las bases de datos con las que se cuente, lo cual puede ser definido como se describe en el siguiente cuadro:

Riesgo de vulneración de datos personales	Definición
Muy alto	Si el factor de riesgo está materializado y no depende de la probabilidad. Si hay constancia de diversas materializaciones de dicho riesgo en el último año en el Instituto de la Juventud Regia en cualquiera de sus coordinaciones y/o áreas. Si hay constancia de una materialización de dicho riesgo en el último año en el Instituto de la Juventud Regia en cualquiera de sus coordinaciones y/o áreas. Existen auditorías o estudios que identifican importantes vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.
Alto	Cuando se materializó el riesgo en el último año en el instituto de la juventud regia en cualquiera de sus coordinaciones y/o áreas. Existen estudios que determinan que la probabilidad podría ser alta. Existen auditorías o estudios que identifiquen posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes.

Baja	Antecedente de una materialización de dicho riesgo en los últimos 10 años en el instituto de la juventud regia en cualquiera de sus coordinaciones y/o áreas.
Improbable	Cuando no exista evidencia de la materialización de dicho riesgo en ningún caso.

Ahora bien, por cada tratamiento de datos personales se solicita diversa información conformando las bases de datos con que se cuenta, por lo que a continuación se presentan los niveles de riesgo de acuerdo al tipo de datos personales que se trata en posesión del Instituto de la Juventud Regia en cualquiera de sus coordinaciones y/o áreas cómo se refiere a continuación:

Tipo de información	Nivel de Riesgo
Documentos personales: • Correos electrónicos • Actas de nacimiento • Curp • Identificaciones • Documentos académicos • Documentos patrimoniales • Entre otros.	Medio
Aspectos personales: • Personas o grupos con los que se relaciona • Temperamento • Carácter • Inteligencia • Roles sociales • Capacidad de adaptación • Tolerancia al riesgo • Gustos/preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales, ...) • Cuidado de salud • Culturales (lectura. música, arte, ...) • Pertenencia y actividades en asociaciones sociales y culturales • Entre otros	Alto
Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos:	Bajo

• Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc. • Hábitos de consumo • Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales,...) • Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.) • Entre otros	
Rendimiento laboral: • Control de acceso al lugar de trabajo • Grabación de imágenes en zonas de acceso o en oficinas • Grabación de audio en zonas de acceso o en oficinas. • Monitorización de los equipos de los empleados • Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos) • Entre otros	Medio
Situación económica: • Renta personal • Ingresos mensuales • Patrimonio (bienes/ inmuebles) • Entre otros.	Medio
Estado financiero: • Solvencia financiera • Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; • Nivel de deuda (Préstamos personales, hipotecas) • Ingresos • Entre otros.	Muy Alto
Información Bancaria: • Cuentas bancarias. • Tarjetas. • Entre otros.	Muy Alto
Datos de comportamiento de empleados: • Fiabilidad de la persona • Hábitos y valores que facilitan la convivencia	Medio

• Hábitos y valores que facilitan el trabajo y el estudio • Hábitos y valores que influyen en el bienestar personal, laboral y familiar • Hábitos y valores que influyen en el compromiso con las personas y con la sociedad • Estabilidad laboral. • Antecedentes de comportamiento. • Entre otra información.	
Datos de localización: • Registro de desplazamientos • Registro de lugares habituales • Registro de rutinas en base a localización • Registro de lugares habituales	Medio
Datos de Salud: • Historia clínica • Informes de salud • Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales • Recetas médicas • Datos relativos a la salud física • Datos relativos a la salud mental • Datos relativos a prestación de servicios de atención sanitaria • Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido) • Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. • Datos Genéticos	Alto
Datos biométricos: • Huella dactilar • Facciones rostro • Iris • Venas de la palma de la mano • Voz • Oreja • Gestos • Modo de andar • Descriptores corporales de cualquier índole • Trazos (firma)	Alto

Categorías especiales de datos o que permitan inferirlos: • Origen étnico • Origen racial • Opiniones políticas • Convicciones religiosas • Convicciones filosóficas • Afiliación sindical • Datos relativos a la salud • Datos relativos a la vida sexual • Datos relativos a las orientaciones sexuales • Entre otros.	Alto
Datos personales relativos a probables delitos e infracciones administrativas	Muy Alto
Metadatos: • Datos de tráfico de las comunicaciones electrónicas • Identificación de emisor y/o receptor en las comunicaciones • Datos en conexiones a internet: localización, características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logrado, conexión (IP, proveedor de servicios, velocidad de descarga). • Entre otros.	Medio
Datos de Identificación: • Nombre • Estado Civil • Fecha de Nacimiento • Nacionalidad • Lugar de nacimiento • Domicilio Teléfono • Correo electrónico • Firma autógrafa • Firma electrónica • Edad • Imagen	Bajo

Por lo que toca a los tratamientos relacionados a los menores de edad, personas adultas mayores, personas en situación de vulnerabilidad, víctimas discapacitadas, etc., se analiza el riesgo de la información personal de acuerdo al siguiente cuadro:

Categoría de Titular / Factor de riesgo	Nivel de riesgo
Menores de 14 años	Reforzado
Víctimas de violencia de género	Reforzado
Menores dependientes de sujetos vulnerables	Reforzado
Personas bajo guardia y custodia de víctimas de violencia de género	Reforzado
Mayores con algún grado de discapacidad	Reforzado
Personas con enfermedades mentales	Reforzado
Discapacitados	Reforzado
Sujetos en riesgo de exclusión social	Reforzado
Pacientes	Alto
Personas mayores	Alto
Personas que acceden a servicios sociales	Medio

En este contexto, una vez evaluado el nivel de riesgo, de los datos personales que se manejan internamente en el Instituto de la Juventud Regia, se establece en la siguiente tabla la probabilidad de que se materialice el impacto de vulnerabilidad con la cantidad de titulares que se establecen en los tratamientos:

Tipo de dato	Nivel de Riesgo Inherente
Información financiera y Bancaria	Reforzado
Titulares de alto Riesgo	Reforzado
Biométricos	Alto
Salud	Alto
Datos sobre la ideología; creencias religiosas, filosóficas o morales; opiniones políticas y afiliación sindical.	Alto
Datos sobre la vida sexual	Alto
Académicos	Medio

Laborales	Medio
Características físicas	Medio
Pasatiempos, entretenimiento y diversión	Bajo
Identificación	Bajo

Ahora, basado en la tabla anterior de los tipos de datos personales que se manejan en las áreas de trabajo del Instituto de la Juventud Regia, es indispensable calcular la probabilidad del riesgo de posibles vulneraciones con valores aproximados de la cantidad de titulares en los cuales el Instituto de la Juventud Regia resguarda su información personal, por lo que se presenta la siguiente tabla calculado el riesgo mencionado anteriormente:

Tipo de dato	Nivel de Riesgo Inherente	Volumen de titulares				
		50	**500**	**5k**	**50k**	**500k**
Información financiera y Bancaria	Alto	4	4	5	5	5
Titulares de alto Riesgo	Alto	4	4	5	5	5
Biométricos	Alto	4	4	5	5	5
Salud	Alto	4	4	5	5	5
Datos sobre la ideología; creencias religiosas, filosóficas o morales; opiniones políticas y afiliación sindical.	Alto	1	2	3	3	3
Datos sobre la vida sexual	Alto	1	2	3	3	3
Académicos	Medio	1	1	2	3	3
Laborales	Medio	1	1	2	3	3
Características físicas	Medio	1	1	1	2	2
Pasatiempos, entretenimiento y diversión	Bajo	1	1	2	2	2
Identificación	Bajo	1	1	1	1	1

A continuación se describen los niveles de riesgo en 5 niveles donde se pretende ver la materialización de una vulneración y afectación que este mismo generaría:

Nivel de riesgo	Casos en los que ocurre
Nivel 1	• El nivel de riesgo inherente de los datos sin importar el número de personas. • El nivel de riesgo es inherente sea alto tengan hasta 500 personas.
Nivel 2	• El nivel de riesgo es inherente sea medio y se tengan hasta 50,00 personas. • El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta 5,000 personas.
Nivel 3	• El nivel de riesgo inherente de los datos sea medio y se tenga 50,000 personas en adelante. • El nivel de riesgo inherente de los datos personales sea alto y se tengan de 5,000 en adelante.
Nivel 4	• El nivel de riesgo inherente de los datos personales es muy alto y se tengan hasta 5,000 personas en adelante.
Nivel 5	• El nivel de riesgo de los datos personales sea muy alto y se tengan más de 50,000 personas.

Con el fin de visualizar la materialización del riesgo de vulneración de los datos personales que se manejan, se presenta la tabla con algunos riesgos que puedan presentarse dentro del Instituto de la Juventud Regia donde se evalúa el riesgo concordando con el tipo de riesgo y tratamiento que se esté contando:

Actividad o Categoría de Datos	Nivel de	Vulnerabilidad	Nivel de Riesgo

impacto			
ACTIVIDADES			
Control de Acceso al Internet • Análisis o evaluación de tiempos de uso de internet. • Control de permisos para actividades de navegación en internet. Entre otros relacionados.	Medio	Vulneraciones a las redes internas así como la información de sitios de navegación de cada servidor, así como los permisos para autorizaciones en la red, lo cual no constituye el ingreso a los servidores donde se almacena la información.	3
Observación: • Vigilancia mediante imágenes • VIgilancia mediante sonidos • Vigilancia mediante comunicaciones • Vigilancia de Internet Entre otros relacionados.	Alto	Vulneración a la vigilancia de las instalaciones y centros de la juventud del Instituto de la Juventud Regia así como las comunicaciones oficiales.	3
Control físico de acceso: • Control de acceso a las instalaciones • Control de Acceso a los eventos • Control de Acceso a las áreas específicas Entro otros que estén relacionados.	Bajo	Acceso de personas no autorizadas a la información de quienes accedan a las instalaciones o quienes acuden a los eventos del Instituto de la Juventud Regia	1
Decidir sobre o impedir el ejercicio de derechos fundamentales: • Derecho a la igualdad • Derecho a la no discriminación • Derecho a la vida y la	Alto	Vulneración a los procesos que se llevan a cabo en el Instituto de la Juventud Regia referente a solicitudes, servicios,	3

integridad física • Derecho a la libertad religiosa • Derecho a la libertad personal • Derecho al patrimonio • Derecho a la intimidad personal y familiar • Derecho a la propia imágen • Derecho a la libertad de expresión e información • Derecho a la libertad de cátedra • Derecho a la libertad de reunión • Derecho a la libertad de asociación • Derecho al libre acceso a cargos y funciones públicas en condiciones de igualdad • Derecho a la igualdad penal • Derecho a la educación • Derecho a la libertad sindical • Derecho de petición Otros derechos relacionados consagrados en la Constitución Política de los Estados Unidos Mexicanos.		procedimientos, dudas o quejas, así como cualquiera que se encuentre dentro de las facultades del Instituto.	
Decidir sobre el control del interesado de sus datos personales: • Derecho de acceso • Derecho de rectificación • Derecho de oposición • Derecho de Cancelación • Derecho de la portabilidad	Alto	Privar los derechos de los titulares en materia de datos personales.	3
Decidir sobre el acceso a un servicio de los cuales el Instituto de la Juventud Regia presta.	Alto	Vulnerar la necesidad de un servicio municipal, de	3

		las y los ciudadanos al solicitar un servicio.	
Decidir sobre la realización o ejecución de un contrato laboral como de proveedores.	Alto	Riesgo de que no se materialice el trabajo o el servicio por fuga de información	2
Conservación con fines de archivo	Medio	Vulneración a toda la información o pérdida de la misma en archivos físicos como electrónicos.	3
DATOS PERSONALES			
Documentos Personales: • Correos electrónicos • Actas de Nacimiento • CURP • Identificaciones • Documentos académicos • Documentos patrimoniales • Entre otros.	Medio	Vulneración a la información personal de identificación, académica y patrimonial de usuarios y servidores públicos.	3
Aspectos Personales: • Personas o grupos con los que se relaciona • Temperamento • Carácter • Inteligencia • Redes Sociales • Capacidad de adaptación • Tolerancia de riesgo • Gustos/ preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales,...) • Cuidado de Salud • Culturales (lectura, música, arte,...) • Pertenencia y actividades en asociaciones sociales y culturales • entre otros.	Alto	Vulneración a los datos que identifican a las personas de acuerdo a sus aspectos personales, pudiendo catalogar a las personas de acuerdo a sus intereses personales.	3

Preferencias de consumos, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos: • Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc. • Hábitos de consumo • Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, redes sociales,...) • Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.) • Entre otros.	Bajo	Vulneración a los intereses de las personas lo cual pudiera ocasionarles el ser víctimas de fraudes o extorsiones, por el conocimiento de sus hábitos, preferencias gustos, necesidades, etc.	1
Situación económica: • Renta personal • Ingresos mensuales • Patrimonio (bienes muebles/ inmuebles) • Situación laboral • Entre otros	Medio	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorsiones	3
Estado Financiero: • Solvencia financiera • Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc; • Nivel de deuda (préstamos personales, hipotecas) • Ingresos • Entre otros.	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorsiones.	5
Datos de Salud: • Historia clínica • Informes de salud • Informes de baja laboral	Alto	Pueden ser objeto de ataques a la privacidad personal, discriminación,	3

por motivos de salud para el Servicio de Prevención de Riesgos Laborales • Recetas médicas • Datos relativos a la salud física • Datos relativos a la salud mental • Datos de la prestación de servicios de atención sanitaria • Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido) • Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente • Datos Genéticos.		manipulacion, o perjuicio moral.	
Categorías especiales de datos o que permitan inferirlos: • Origen étnico • Origen racial • Opiniones políticas • Convicciones religiosas • Convicciones filosóficas • Afiliación sindical • Datos relativos a la salud • Datos de la vida sexual • Datos relativos a las orientaciones sexuales • Entre otros	Alto	La vulneración de esta información personal tenería consecuencias morales y sociales ya que pueden ser objeto de discriminación si se difunde esta información o si se tiene accesos no autorizados.	3
Datos de Identificación: • Nombre • Estado civil • Fecha de nacimiento • Nacionalidad • Lugar de nacimiento • Domicilio	Bajo	Acceso no autorizado a información del personal del Municipio y sus Paramunicipales, o bien a la información de las personas	1

• Teléfono • Correo electrónico • Firma autógrafa • Firma electrónica • Edad • Imagen		usuarias, valorándose su información personal de identificación y contacto.	
Categoría de Titular/ Factor de Riesgo			
Menores de 14 años	Muy Alto	Vulneración a información de menores de edad.	5
Menores dependientes de sujetos vulnerables	Muy Alto	Se pondría en riesgo la identidad de estas personas así como las necesidades, pudiendo ser víctimas de algún delito.	4
Mayores con algún grado de discapacidad	Muy Alto	Vulneración de su información personal sensible.	4
Personas con enfermedades mentales	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	4
Discapacitados	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	4
Pacientes	Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	3
Personas Vulnerables: • En situación de especial vulnerabilidad • Existe un desequilibrio	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de	4

entre la posición del titular y del responsable.		discriminación.	

IV. ANÁLISIS DE BRECHA

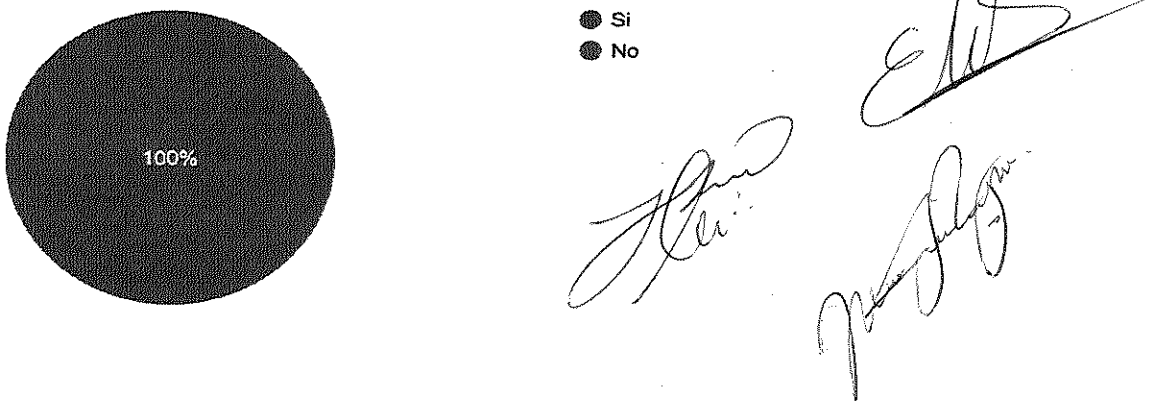
Para poder realizar el análisis de brecha, el Instituto de la Juventud Regia realizó y aplicó un cuestionario con el objetivo de evaluar un auto diagnóstico que muestre el rendimiento del desempeño esperado en las medidas de seguridad empleadas por las áreas generadoras de datos personales. Las preguntas establecidas para evaluar el entorno del rendimiento de la protección de los datos personales fueron las siguientes:

1. ¿Pones atención en no dejar a la vista información personal y llevar registro de su manejo? por ejemplo: en el escritorio o en algún otra área)
2. ¿Tienes mecanismos para eliminar de manera segura la información (Por ejemplo: borrado de archivos electrónicos, etc)
3. ¿Haz establecido y documentado los compromisos respeto a la protección de datos?(Conoces la materia y organizas la información)
4. ¿Realizas respaldos periódicos de los datos personales? (Por ejemplo: Haces respaldo de la información que manejas en la nube, en USB o disco duro externo)
5. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico? (Por ejemplo: filtro de seguridad en entrada, acceso restringido al público en general o al personal que no es del área)
6. ¿Realizas actualizaciones al equipo de cómputo? (Asegurarse que el personal de sistemas realice las actualizaciones necesarias a tu equipo)
7. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?(Ejemplo: tener contraseñas en el equipo de computo)¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico? (Ejemplo: tener contraseñas en el equipo de computo)
8. ¿Cuidas el movimiento de información en entornos de trabajo digitales? (Por ejemplo: Comunicas la información digital de tus labores)

A continuación se muestran los resultados de las preguntas aplicadas a los servidores públicos del Instituto de la Juventud Regia:

¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo? (Por ejemplo: en el escritorio o en algún otra área)

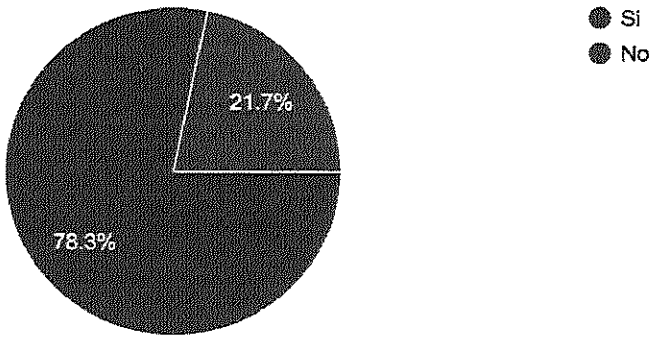
23 responses



¿Haz establecido y documentado los compromisos respeto a la protección de datos? (Conoces la

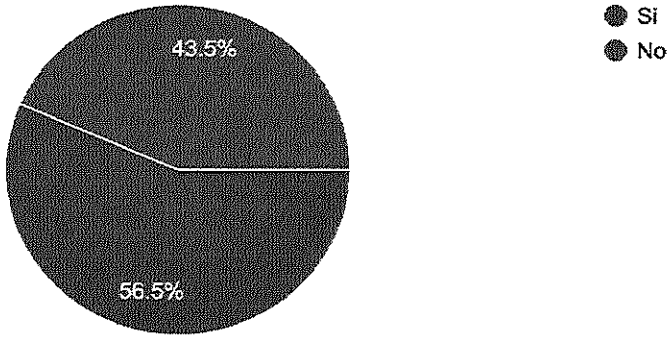
¿Tienes mecanismos para eliminar de manera segura la información (Por ejemplo: borrado de archivos electrónicos, etc)

23 responses

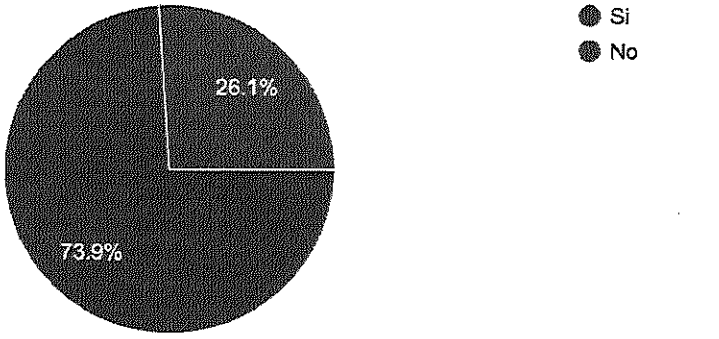


¿Realizas respaldos periódicos de los datos personales? (Por ejemplo: Haces respaldo de la información que manejas en la nube, en USB o disco duro externo)

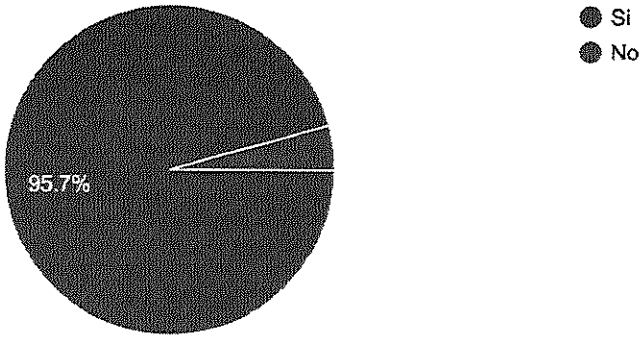
23 responses



¿Tienes medidas de seguridad para acceder al entorno de trabajo físico? (Por ejemplo: filtro de seguridad en entrada, acceso restringido al público en general o al personal que no es del área)
23 responses

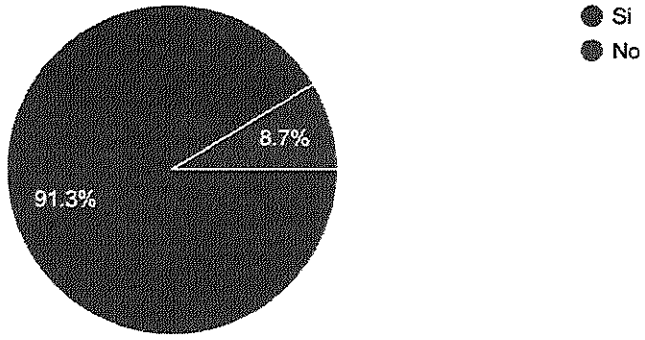


¿Cuidas los movimientos de información en entornos de trabajo físico? (Ejemplo: que solamente tenga acceso a la información personal autorizado)
23 responses



¿Cuidas el movimiento de información en entornos de trabajo digitales? (Por ejemplo: Comunicas la información digital de tus labores)

23 responses



Con estos resultados en mano, demuestra que existe un buen desempeño en las actividades de los servidores públicos del Instituto de la Juventud Regia, a excepción de un ligera brecha de peligro en los respaldos por lo que se propone resaltar el compromiso del plan de trabajo que este documento presenta.

V. PLAN DE TRABAJO

La existencia de este documento de seguridad busca poder resaltar el compromiso y los deberes que el Instituto de la Juventud Regia cuenta para la máxima protección de los datos personales que se generan en las distintas áreas que conforman la dependencia. Debido a su importancia actual de los datos personales, se debe de mantener actualizado el plan de trabajo que permite poder alcanzar los objetivos en el sistema de seguridad de protección de datos personales.

La finalidad del plan de trabajo es poder visualizar de una manera más amplia, las actividades o medidas que el Instituto de la Juventud Regia realiza para la aplicación del presente documento de seguridad.

Esto, se realizará con base a las atribuciones que vienen establecidas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Nuevo León.

Para la ejecución del presente plan de trabajo, se implementará lo siguiente:

1. Se comunicará a la Contraloría Municipal la emisión del documento seguridad y, se dará difusión en versión pública para el debido tratamiento de los datos personales al interior de las áreas del Instituto de la Juventud Regia, de los lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Monterrey.
2. Dar continuidad a los planes anuales de capacitación en materia de protección de datos personales que maneje la Contraloría Municipal del Municipio de Monterrey

dirigido a todos los servidores públicos que laboren en el Instituto de la Juventud Regia para que sean capacitadas y mejorar el conocimiento de los principios y deberes que rigen la materia, así como crear conciencia de la protección de la información.

3. Mantener actualizados los avisos de privacidad e inventarios de datos personales.

Además del plan de trabajo, se implementarán las siguientes medidas de protección:

VI. MEDIDAS DE SEGURIDAD EN LA ADMINISTRACIÓN PÚBLICA MUNICIPAL CENTRALIZADA Y LAS DEPENDENCIAS PARAMUNICIPALES DE MONTERREY.

Medidas de seguridad físicas y administrativas

Las Dependencias de la Administración Pública Municipal Centralizada y las Entidades Paramunicipales, deberán implementar como mínimo las siguientes **medidas generales de seguridad física**, para evitar daños, sustracciones o intromisiones no autorizadas en las instalaciones y archivos de información del sujeto obligado:

I. En la medida de lo posible asignar un espacio seguro y adecuado para el tratamiento de datos personales, que no se encuentre a la vista del público y que preferentemente no sea un área de paso frecuente por el personal del trabajo o ajeno al mismo.
II. Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.
III. Evitar que se dejen descuidados o sin la atención debida documentos que contengan datos personales.
IV. Establecer un plan de contingencia con protocolos de seguridad, que incluya, cuando menos, la designación de responsables por piso, procedimientos de control, señalizaciones y medidas de protección física contra incendio, inundación, sismo, explosión y cualquier otra forma de desastre natural o humano.
V. Verificar que en ningún caso los documentos que contengan datos personales se utilicen como papel reciclable ni de doble uso, ya que una vez transcurridos los plazos en que deban cancelarse o al tratarse de proyectos no utilizables, deberán ser destruidos.
VI. Implementar programas de capacitación en materia de protección de datos personales al interior del Municipio, y sus Entidades Paramunicipales.

Medidas de seguridad en el entorno

Las Dependencias de la Administración Pública Municipal Centralizada y las Entidades Paramunicipales, deberán adoptar con mínimo las siguientes **medidas de seguridad en el entorno**, para evitar el acceso físico no autorizado a las instalaciones y a su información.

I. Registrar a visitantes que accedan a instalaciones;
II. Portar el gafete de visitante dentro de las instalaciones, por personas ajenas a la Administración Pública Municipal Centralizada y las Paramunicipales;
III. Asegurar el retiro de pases de visita.
IV. Identificar a los servidores públicos adscritos al sujeto obligado, los cuales deberán portar la identificación, deberá ser expedida y firmada por autoridad competente, e incluir cuando menos nombre, cargo y número de empleado, fotografía, nombre de la

registrar a las personas y previa identificación, darle acceso correspondiente con una tarjeta de visitante.

Medidas de Seguridad en caso de desastres naturales:

Incendios y humos: Contar con detectores y sensores contra incendios, humos y gases, en las dependencias de la Administración Pública Municipal, Centralizada y Paramunicipal.

Medidas de seguridad con respecto a la Infraestructura tecnológica:

Con fundamentos en el artículo 116 del Reglamento de la Administración Pública Municipal de Monterrey, la Secretaría de Innovación y Gobierno Abierto, a través de la Dirección General de Gobierno Digital y Soporte Tecnológico es la unidad administrativa encargada de las medidas de seguridad con respecto a:

- Amenazas externas en la red
- Antivirus
- Firewall
- Instalación de software no autorizado
- Servidores y sus copias de seguridad
- Copias de seguridad o respaldos de la información de los servidores

Formas de supresión y borrado seguro de información, cuyo contenido se encuentran inmersos datos personales

Antes de establecer la modalidad de supresión y borrado seguro de la información, es indispensable precisar sobre su ciclo de vida, ya que se conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental al interior del Municipio.

Al tratarse de datos personales contenidos en archivos físicos y en sistemas electrónicos como en la nube, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la fall en los equipos electrónicos o en los sistemas; por ello, el Municipio de Monterrey, cuenta con el apoyo de la Dirección General de Gobierno Digital y Soporte Tecnológico de la Secretaría de Innovación y Gobierno Abierto, quien es la encargada de ejecutar acciones para garantizar la Seguridad de la información.

Al tratarse de datos personales resguardados físicamente, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción.

Físicamente:

1. **Trituración mediante corte cruzado o en partículas**, consiste en cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se pueda unir.
2. **Destrucción de los medios de almacenamiento electrónicos a través de la desintegración**, a fin de que deje de existir la información que se desea eliminar, se separa, completa o parcialmente los elementos que la conforman.

Lógicamente:

1. **Sobre- escritura**, esta consiste en sobre escribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

   Anonimización: Es el reducir al mínimo los riesgos de re identificación de los datos, manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personales, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización, no conlleva una distorsión de los datos reales.

VII. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Se podrán realizar verificaciones aleatorias en las Dependencias y Entidades de la Administración Pública Centralizada y Paramunicipal, para conocer el grado de cumplimiento de las medidas de seguridad.

VIII. PROGRAMA GENERAL DE CAPACITACIÓN

El programa de capacitaciones en materia de protección de datos personales se llevará a cabo acorde al plan anual emitido por la Contraloría Municipal del Municipio de Monterrey, con el objetivo primordial de crear un acercamiento en materia de protección de datos personales para tener una mayor comprensión de la responsabilidad del trabajar con información personal de ciudadanos y trabajadores tanto del Instituto de la Juventud Regia como de la Administración Pública Municipal en general, así también como el informar sobre las medidas de seguridad básicas que se deben de llevar a cabo para proteger la información que contiene datos personales.

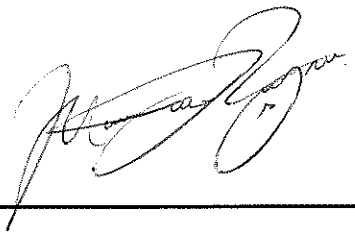
IX. ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará siguiendo las bases en el artículo 42 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, cuando sucedan los siguientes acontecimientos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad,

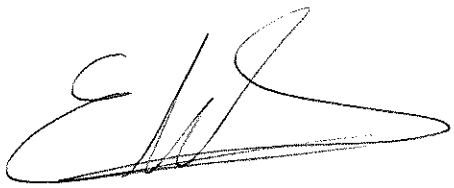
Dado en el Comité de Transparencia del Instituto de la Juventud Regia del Municipio de Monterrey, Nuevo León, a los (12 de Abril de 2024)

COMITÉ DE TRANSPARENCIA DEL INSTITUTO DE LA JUVENTUD REGIA DEL MUNICIPIO DE MONTERREY



MARÍA JOSÉ REYNA GALVAN

PRESIDENTE DEL COMITÉ



ELENA DENISSE VERA VERA

SECRETARIO TÉCNICO DEL COMITÉ

ANDREA ALEJANDRA LANDAVERDE TREJO

VOCAL DEL COMITÉ