consejo para la Transparencia

OFICIO N° 000501

MAT: Formula recomendaciones para el debido cumplimiento de las disposiciones comprendidas en la Ley N°19.628, sobre Protección de la Vida Privada, y las medidas de seguridad que se sugiere adoptar los órganos de la Administración del Estado, en el tratamiento de los datos personales y datos sensibles, con ocasión del brote de COVID-19.

ANT: Oficio N°211, de 17 de marzo de 2020, del Consejo para la Transparencia, que formula recomendaciones en materia de transparencia, acceso a la información y protección de datos personales, para el tratamiento de información por antecedentes vinculados a la enfermedad infecciosa denominada COVID19 o coronavirus.

Santiago, 21 ABR 2020

A: SEGÚN DISTRIBUCIÓN

DE: ANDREA RUIZ ROSAS
DIRECTORA GENERAL
CONSEJO PARA LA TRANSPARENCIA

1. En el contexto de la pandemia global así calificada por la Organización Mundial de la Salud, como consecuencia del brote de COVID-19, también denominado Coronavirus, el Consejo para la Transparencia, mediante Oficio N°211, de 17 de marzo de 2020, formuló recomendaciones a los órganos de la Administración del Estado, en materia de transparencia, acceso a la información y protección de datos personales, para el tratamiento de información y datos relacionados con el coronavirus.

Lo anterior, con el objetivo principal de recordar a la población, en general, y a las instituciones y prestadores de servicios de salud públicos y privados, que los datos personales referidos, vinculados o relacionados a los estados de salud físicos o psíquicos de personas identificadas o identificables constituyen datos sensibles, según establece el artículo 2°, letra g), de la Ley N°19.628, sobre Protección de la Vida Privada (LPVP). Por ello, la divulgación o comunicación de cualquier información concerniente a personas afectadas o eventualmente contagiadas con la enfermedad del COVID-19, debe realizarse dando estricto cumplimiento a la normativa sobre protección de datos personales.

2. Sin perjuicio de lo anterior, esta Corporación ha considerado conveniente disponer de una serie de recomendaciones a los órganos de la Administración del Estado, complementarias de las remitidas anteriormente, que tiendan a orientar a los servidores públicos respecto de la regulación vigente en materia de tratamiento de datos personales, y de aquellos calificados como sensibles.

3. Por lo anterior, y en virtud de la facultad establecida en la letra m) del artículo 33 de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, el Consejo Directivo del Consejo para la Transparencia, en sesión ordinaria N°1.088, de fecha 14 de abril de 2020, acordó remitir a usted el presente Oficio, por el cual se formulan recomendaciones sobre el adecuado tratamiento que los órganos de la Administración del Estado deben otorgar a la información, antecedentes, documentos o las bases estadísticas, que incluyan datos personales y sensibles que le correspondan administrar, en el contexto de la emergencia sanitaria generada por la referida enfermedad, así como las medidas de seguridad de la información que se recomienda implementar, para el debido resguardo de dichos datos.

4. Las presentes recomendaciones tienen como objeto garantizar el adecuado cumplimiento por parte de los órganos de la Administración del Estado de lo dispuesto en el artículo 19 N°4 de la Constitución Política de la República y las normas pertinentes de la ley N°19.628, sobre Protección de la Vida Privada, y sus modificaciones posteriores. A este respecto, deben también considerarse los principios orientadores y criterios jurídicos contenidos en las Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado, publicadas en el Diario Oficial con fecha 14 de septiembre de 2011.

5. El Consejo para la Transparencia advierte que la precariedad y falta de actualización de nuestra regulación en materia de protección de datos personales, constituye un obstáculo en la implementación de medidas adecuadas de resguardo, lo que se manifiesta aún con más fuerza en las circunstancias excepcionales en las que nuestro país se encuentra. Por lo anterior, mediante Oficio N°302, de 9 de abril del presente año, esta Corporación hizo llegar a las autoridades competentes, determinadas propuestas de perfeccionamiento normativo necesarias para subsanar estos vacíos legales.

   Sin embargo, la debilidad de la regulación vigente no puede ser una excusa para que esta Corporación no ejerza las facultades que el ordenamiento jurídico le entrega, si no más

bien constituye la razón y fundamento de las recomendaciones que más adelante se indican.

6. En consecuencia, para los efectos de proceder en conformidad a la Constitución y a la ley en las operaciones de tratamiento de datos personales, que se lleven a efecto por parte de los órganos de la Administración del Estado, en el ámbito de sus respectivas competencias, el Consejo para la Transparencia le informa lo siguiente:

I. MARCO NORMATIVO GENERAL PARA EL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO.

a) **Derecho fundamental a la protección de datos personales.** El derecho a la protección de los datos personales está consagrado en el artículo 19 N°4 de la Constitución Política de la República, el cual consiste en la facultad que tiene cada individuo de controlar el flujo de informaciones que le conciernen, esto es, sus datos personales. Por su parte, la Ley N°19.628, sobre Protección de la Vida Privada (en adelante LPVP), establece que el tratamiento de los datos personales sólo puede efectuarse cuando el titular consiente expresamente en ello por escrito, o la ley lo autorice.

b) **Definición de dato personal.** Según establece el literal f) del artículo 2° de la LPVP, los datos de carácter personal son aquellos *"relativos a cualquier información concerniente a personas naturales, identificadas o identificables."*.

Sin embargo, es importante tener presente que existen ciertas categorías de datos, sujetos a reglas especiales, denominados "datos sensibles", cuyo marco normativo específico será abordado en el punto II. del presente Oficio.

c) **Tratamiento de datos personales por organismos públicos.** El artículo 20 de la LPVP contiene una habilitación o autorización a los organismos públicos para tratar datos personales respecto de las materias de su competencia, sin el consentimiento del titular. Para ello, la norma dispone expresamente que dichos tratamientos deben sujetarse a las reglas contenidas en la misma ley, entre las que destacan:

Principios rectores del tratamiento de datos personales	Tratamiento legítimo por parte de los órganos de la Administración del Estado
Principio de licitud	Respecto al tratamiento de datos personales por parte de organismos públicos, el artículo 20 de la referida ley dispone que "sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes.". Cumpliendo estas condiciones, los organismos públicos no requieren del consentimiento del titular de los datos. De ahí que resulta indispensable establecer con precisión y antes de iniciar cualquier procesamiento de datos, el marco normativo que

	habilita a un determinado organismo público a efectuar operaciones específicas de tratamiento de información de carácter personal, incluyendo su eventual comunicación a terceras entidades, sean públicas o privadas.
Principio de finalidad	Según dispone el inciso primero del artículo 9° de la Ley N°19.628, las operaciones de tratamiento que se realicen respecto de datos personales deberán circunscribirse estrictamente a los fines para los cuales hubieran sido inicialmente recolectados. En el caso de los órganos públicos, la referida finalidad estará determinada en función de las materias propias de su competencia, definidas en sus leyes especiales.
Principio de proporcionalidad	Sólo pueden tratarse aquellos datos necesarios para conseguir los fines que justifican su recolección. Por ejemplo, se entenderá que se cumple con el principio de proporcionalidad cuando la comunicación y posterior procesamiento de los datos sea adecuada y conducente para la consecución de los objetivos planteados, y no excesiva, teniendo presente el tipo y cantidad de datos que son traspasados.
Principio de información	De acuerdo con lo dispuesto en los artículos 3°, 4°, 13 y 20 de la Ley N°19.628, los organismos públicos deberán informar al titular, de forma previa a la recolección de los datos, acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con su tratamiento, de la posible comunicación a terceros y de los derechos que pueden ser ejercidos por ellos. Lo anterior, deberá efectuarse poniendo a disposición de los titulares de los datos una adecuada política de privacidad.

II. MARCO NORMATIVO ESPECIAL PARA EL TRATAMIENTO DE DATOS SENSIBLES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO.

a) **Concepto de datos sensibles.** La LPVP identifica una categoría especial de datos personales denominados "datos sensibles", que son definidos —en el literal g) del artículo 2°— como *"aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."*.

b) **Alcance del concepto.** Al tratarse de una definición legal de carácter abierto, el concepto de dato personal sensible puede abarcar aspectos tan disimiles como la información médica de las personas, los registros de navegación en internet, su

orientación sexual, por mencionar sólo algunos. De esta manera, al momento de calificar un dato personal como sensible, los organismos públicos deben tener presente, al menos, las siguientes categorías:

i. **Datos que se refieren a características físicas de una persona**, tales como datos biométricos, muestras y datos biológicos, datos de salud ya sea física, psíquica; datos sobre estados de ánimo, entre otros.

ii. **Datos que se refieren a características morales de una persona**, tales como información sobre orientación o preferencia sexual, creencias o convicciones religiosas, éticas o políticas, entre otros de similar naturaleza.

iii. **Datos que se refieren a hechos o circunstancias de su vida privada o intimidad**, tales como los hábitos personales, la información sobre desplazamiento geográfico, la geolocalización, la navegación en internet, sus redes de amistad y contacto, entre otros.

c) **Condiciones de licitud para el tratamiento de datos personales sensibles.** Conforme dispone el artículo 10 de la LPVP, existe una prohibición general de tratamiento de datos personales sensibles salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

De esta forma, los organismos públicos únicamente podrían tratar datos personales sensibles cuando concurra alguna de las siguientes circunstancias:

Habilitante del tratamiento o base de licitud	Ámbito de aplicación
Autorización legal	La propia LPVP entrega una autorización genérica para el tratamiento de datos personales por parte de organismos públicos que realicen respecto de las materias de su competencia y cumpliendo además las reglas pertinentes contenidas entre los artículos 1 y 19 de la misma ley. Sin embargo, respecto del tratamiento de datos personales sensibles, cada organismo público debe examinar si cuenta con habilitación legal expresa en las normas que regulan su funcionamiento, establezcan sus competencias o determinen sus funciones especiales. De ser así, el tratamiento de datos personales sensibles tendrá su fundamento legal en esa regla expresa. Ahora bien, en aquellos casos donde no exista tal regla expresa, el tratamiento de datos personales sensibles podría basar su habilitación legal en la regla general del artículo 20, sí y sólo sí el tratamiento de esta categoría especial de datos resulta

	imprescindible para el debido cumplimiento de su función pública, forme parte esencial de las materias de su competencia y se efectúe con pleno respeto a las reglas contenidas entre los artículos 1 y 19 de la LPVP. Si no fuera el caso, el organismo público no podrá tratar datos personales sensibles, a menos que obtenga consentimiento expreso del titular o que sea necesario para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares de dichos datos, caso este último que cobra especial relevancia atendida la situación de pandemia que vive el país.
Consentimiento	Si un organismo público requiere tratar datos personales sensibles y no cuenta con la habilitación legal que exige el artículo 10 de la LPVP, podrá hacerlo obteniendo el consentimiento previo y expreso del titular, en los términos establecidos en el artículo 4° de la LPVP, cumpliendo además de manera estricta con la regla del artículo 20 que establece que ese tratamiento "sólo podrá efectuarse respecto de las materias de su competencia" e informando adecuadamente sobre la finalidad de la captura de datos, su procesamiento y eventual comunicación.
Determinación u otorgamiento de beneficios de salud	Finalmente, el artículo 20 de la LPVP establece una regla especialísima respecto del tratamiento de datos personales sensibles cuando sean necesarios para la determinación u otorgamiento de beneficios de salud para el titular. En el caso de organismos públicos, la aplicación de esta regla tiene un alcance limitado, toda vez que únicamente podrán hacer uso de esta disposición aquellos organismos públicos que otorguen "beneficios de salud" en el ejercicio de sus funciones y respecto de materias de su competencia, conforme dispone el artículo 20 de la LPVP.

d) **Regulación especial aplicable a los datos de salud.** Sin perjuicio de lo expuesto previamente, la normativa vigente contempla una regulación específica aplicable a esta categoría especial de datos sensibles. Sobre el particular, y en especial en el marco de la pandemia global a consecuencia del brote de COVID-19, y en consideración de las circunstancias excepcionales del Estado de Excepción Constitucional de Catástrofe vigente, hay que tener presente las siguientes consideraciones.

e) **Marco legal específico contenido en la Ley Orgánica del Ministerio de Salud.**

En particular, el numeral 5, del artículo 4 del decreto con fuerza de ley N°1, del 2005, del Ministerio de Salud, que fija texto refundido, coordinado y sistematizado del

decreto ley N° 2.763, de 1979 y de las leyes N° 18.933 y N° 18.469, en adelante, Ley Orgánica del Ministerio de Salud, faculta expresamente a dicha Secretaría de Estado a **tratar datos personales o sensibles con el fin de proteger la salud de la población** o para la determinación y otorgamiento de beneficios de salud. Para ello, se indica que podrá requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria. **Todo lo anterior, conforme a las normas de la Ley N°19.628 y aquellas sobre secreto profesional.**

A su vez, el artículo 134 bis del mismo cuerpo legal indica a dicho respecto que los prestadores de salud, las instituciones de salud previsional, el Fondo Nacional de Salud (FONASA) u otras entidades, tanto públicas como privadas, que elaboren, procesen o almacenen datos de origen sanitario podrán efectuar las operaciones de tratamiento de datos que en dicha disposición se señalan (vender, ceder o transferir, a cualquier título), sin el consentimiento del titular, tratándose del otorgamiento de los beneficios de salud que les correspondan, así como del cumplimiento de sus respectivos objetivos legales.

Dado lo anterior, y lo cual resulta plenamente aplicable en las circunstancias sanitarias actuales, el Ministerio de Salud no requiere del consentimiento del titular para llevar a efecto las operaciones de tratamiento de datos de salud, cuando éstas se efectúen con la finalidad de proteger la salud de la población.

Asimismo, tampoco requerirán de aquel consentimiento, los prestadores de salud, las instituciones de salud previsional, el Fondo Nacional de Salud u otras entidades, tanto públicas como privadas, que elaboren, procesen o almacenen datos de origen sanitario, cuando se trate del cumplimiento de sus respectivos objetivos legales.

Con todo, en el ejercicio de esta actividad, se deberá dar pleno cumplimiento a las disposiciones contenidas en la Ley N°19.628, sobre Protección de la Vida Privada. En especial, aquella normativa relativa a la finalidad del tratamiento, información al titular, el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición), cuando corresponda.

Así también, los órganos competentes responsables del tratamiento de datos personales y sensibles deben adoptar las medidas de seguridad de la información personal para garantizar la **integridad, confidencialidad y disponibilidad** de los datos contenidos en sus registros, con la finalidad de evitar la alteración, pérdida y acceso no autorizado de los mismos, especialmente en atención a las especiales circunstancias que vive el país. **El punto III. del presente Oficio abordará esta última materia.**

f) **Regulación relativa al tratamiento de información sensible contenida en la Ley N°20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, y su reglamento aprobado por el decreto N°38, del 2012, del Ministerio de Salud.**

Por otra parte, **tratándose en específico de los datos de salud que se encuentran contenidos en la ficha clínica**, el marco legal para su tratamiento está dado por las disposiciones de la Ley N°20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, y su reglamento aprobado por el decreto supremo N°38, del 2012, del Ministerio de Salud.

Conforme a ello, y según se indicara con antelación en el citado Oficio N°211, de esta Corporación, el principal objetivo de dicha normativa consiste en resguardar la privacidad y la confidencialidad de los datos y muestras de los pacientes, estableciendo diversas salvaguardas respecto de la utilización de los datos contenidos en fichas clínicas.

En particular, **se establece la reserva de la información contenida en la ficha clínica, disponiéndose que toda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como dato sensible**, de conformidad con lo dispuesto en la letra g) del artículo 2° de la ley N°19.628.

A dicho respecto, se establece también que los terceros que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica, lo que incluye al personal de salud y administrativo del mismo prestador, no vinculado a la atención de la persona.

Sin perjuicio de lo anterior, la información contenida en la ficha puede ser entregada, total o parcialmente:

(i) a su titular o representante legal;

(ii) a un tercero autorizado por el titular, mediante poder simple otorgado ante notario;

(iii) a los tribunales de justicia;

(iv) a los fiscales del Ministerio Público y a los abogados, previa autorización del juez competente; y

(v) al Instituto de Salud Pública, en el ejercicio de sus facultades.

Con todo, estas personas e instituciones deberán adoptar las medidas necesarias para asegurar la reserva tanto de la identidad del titular de la ficha clínica como de los datos sensibles contenidos en ella, junto con garantizar que esta información sea utilizada exclusivamente para los fines para los cuales fue requerida.

g) **Comunicación de datos de salud en el marco de la emergencia sanitaria: atribución de la autoridad sanitaria se encuentra circunscrita a comunicar datos a**

determinadas instituciones públicas, para el control del orden y la seguridad sanitaria.

El numeral 5 del artículo 4 de la Ley Orgánica del Ministerio de Salud ya mencionado, se refiere a la facultad de dicha cartera de Estado para "tratar datos personales y sensibles"; luego, la frase final de dicho numeral precisa que dicho tratamiento deberá efectuarse en conformidad a las normas de la Ley N°19.628.

Ante ello, y para determinar qué operaciones se encuentran comprendidas en la autorización legal conferida al Ministerio de Salud, hay que remitirse a la definición que la Ley N°19.628 establece. Así, de acuerdo con lo dispuesto en el literal o) del artículo 2° de dicha ley, se entiende por **"Tratamiento de datos"**: cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

En consecuencia, la autoridad sanitaria, en circunstancias normales, y por cierto en estas circunstancias excepcionales, podrá por una parte, requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria para proteger la salud de la población – incluso tratándose de información que se encuentre contenida en la ficha clínica -, y comunicar dichos datos sensibles, cuando dicha operación de tratamiento se efectúe exclusivamente para el cumplimiento de la finalidad recién mencionada y sólo a aquellos que se encuentren expresamente autorizados por la ley.

De ahí que, en el marco de la pandemia por el brote de COVID-19, y en conformidad con lo dispuesto en el artículo 8° del Código Sanitario, dicha autorización de comunicación sólo alcanzará para poner en conocimiento de las Fuerzas de Orden y Seguridad la información sensible necesaria para cumplir con la finalidad señalada previamente. En otras palabras, la autoridad sanitaria respectiva, sólo podrá comunicar aquellos datos de salud necesarios para ejercer las facultades de control del orden público a la respectiva unidad policial con jurisdicción en la localidad de la cual se trate.

Finalmente, y en aplicación de lo dispuesto en el artículo 7° de LPVP, las Fuerzas de Orden y Seguridad Pública, no podrán, bajo ninguna circunstancia, comunicar los datos sensibles recibidos de la autoridad sanitaria ni efectuar ningún otro tipo de tratamiento respecto de éstos, sino sólo aquél que fuese estrictamente necesario para dar cumplimiento a sus atribuciones constitucionales y legales, respetando siempre el principio de finalidad, seguridad y proporcionalidad en el tratamiento de la información personal sensible de que se trata.

Deberán, además, una vez superadas las circunstancias de emergencia sanitaria, y así declarado oficialmente por la autoridad competente, proceder a la

eliminación de toda aquella información recibida con ocasión de este marco de excepción.

Lo anterior, en conformidad con lo dispuesto en el artículo 19 N°4 de la Constitución Política de la República, que otorga reconocimiento constitucional a la protección de los datos personales y establece que el tratamiento y protección de éstos se efectuará en la forma y condiciones que determine la ley; a lo dispuesto en la Ley N°19.628, y en particular, de acuerdo con lo prescrito en la Ley Orgánica del Ministerio de Salud; el Código Sanitario y sus reglamentos y en la Ley N°20.584 y su reglamento; y, en el Dictamen N°6.785, de 24 de marzo de 2020, de la Contraloría General de la República, mediante el cual precisa que compete a las autoridades expresamente habilitadas por la Carta Fundamental adoptar medidas que afecten derechos constitucionales en el Estado de Excepción de Catástrofe.

h) **Responsabilidad legal y administrativa derivada de la contravención de las normas explicadas previamente.**

Se hace presente que cualquier contravención a lo dispuesto en los párrafos precedentes, dará lugar a la responsabilidad legal establecida en el artículo 23 de la Ley N°19.628, debiendo el órgano público o la persona natural o jurídica privada de que se trate, indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

Así también, el tratamiento no autorizado de datos personales y sensibles por parte de un órgano de la Administración del Estado, en infracción de las disposiciones legales ya señaladas, dará lugar a las responsabilidades administrativas que correspondan. A dichos efectos y de tomar conocimiento de alguna infracción a la legislación citada, el Consejo para la Transparencia remitirá los antecedentes a la Contraloría General de la República para que dicho Ente Contralor persiga las eventuales responsabilidades y adopte las medidas que estime pertinentes.

III. RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN EN EL TRATAMIENTO DE DATOS PERSONALES Y SENSIBLES POR LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO.

Los organismos públicos responsables del tratamiento de datos personales y sensibles, deben adoptar todas las medidas, tanto organizativas como técnicas, que garanticen la **integridad, confidencialidad y disponibilidad,** y en general, la seguridad de todos los datos contenidos en sus registros, con la finalidad de evitar la alteración, pérdida y acceso no autorizado a los mismos.

En consecuencia, con el objeto de dar cumplimiento a la premisa previamente señalada, se recomienda al menos, las siguientes medidas:

Recomendaciones de seguridad de la información	Medidas técnicas que se sugiere implementar al efecto
Garantizar en todo momento la seguridad de esta información, mediante el uso de sistemas informáticos actualizados y protegidos.	1) Incorporar, planificar e implementar controles de Protección de Datos Personales y controles para la Seguridad de la Información. 2) Realizar una clasificación de la información y garantizar un almacenamiento adecuado, según los criterios de seguridad. 3) Establecer procedimientos, planes y políticas de almacenamiento, conservación, recuperación y borrado es esencial para garantizar la seguridad. 4) Conservar los datos solo el tiempo que sea necesario, al momento de eliminar los datos, se debe garantizar ejecutar un procedimiento adecuado de "Borrado Seguro". 5) Tener una política de contraseñas (complejas y con expiración). 6) Para el caso de seguridad perimetral, se recomienda el uso de Firewall de nueva generación, con alta disponibilidad (al menos un Firewall de backup), con protección de amenazas avanzadas, análisis de tráfico y monitoreo. 7) En el caso que se utilice firma electrónica avanzada, se recomienda el uso de dispositivo HSM (Hardware Security Module o Módulo de Seguridad Hardware), que asegure el almacenamiento de firmas electrónicas, certificados digitales, llaves criptográficas, entre otras. 8) Uso de antivirus y antimalware, con actualización permanente. 9) Plan de actualización de servidores, estaciones de trabajo y dispositivos conectados, tanto para sistemas operativos como aplicaciones instaladas.
Incorporar procedimientos para la prevención de filtraciones y accesos indebidos; y la definición de perfiles de acceso a los bancos de datos.	1) Los **sistemas que manejen datos sensibles** deben restringir el acceso a la información sensible, enmascarando o seudonimizando la información. Solo deben tener acceso solo aquellos usuarios, donde exista un fundamento con base jurídica y/o que sea el responsable de la gestión y/o tratamiento de los datos personales.

	2) Todos los organismos deben seguir el **principio del mínimo privilegio**. 3) Establecer una política de control de acceso a sistemas y sectores restringidos. 4) Establecer un procedimiento de gestión de ambientes, para desarrollo de aplicaciones. 5) Acceder externamente a la red interna del organismo solo a través de VPN y realizar gestión en el acceso de VPN. 6) Aislar redes WiFi de uso de externos a la institución.
Informar a los titulares de datos personales sensibles, de las eventuales brechas de seguridad que pudieran ocurrir, de las posibles consecuencias de estas vulneraciones y de las medidas de solución o resguardo adoptadas.	1) Se recomienda generar un plan para la gestión de los incidentes de fuga de información, que considere la detección, alerta, un diagnóstico de la situación, coordinación y ejecución de acciones. 2) Se recomienda tener procedimientos que especifiquen cuándo y a qué autoridades se deben contactar y cómo se deberían informar los incidentes de seguridad de la información. En el caso de los órganos de la Administración del Estado, deben informar al CSIRT de las eventuales brechas de seguridad.
En aquellos casos en que los datos recolectados sean comunicados o transmitidos a terceras personas, naturales o jurídicas, se recomienda la adopción de medidas de encriptación, a efectos de asegurar la integridad y confidencialidad de los datos entre remitente y destinatario.	1) Se debe aplicar la minimización de datos, es decir, intercambiar la información estrictamente necesaria para el cumplimiento del objetivo del intercambio. Cuando la información contenga **datos personales sensibles**, se recomienda que el tránsito de los datos sea encriptados en el origen. 2) Para el intercambio de datos confidenciales, reservados o con datos personales que se realiza a través de correo electrónico, se recomienda encriptar y/o comprimir los datos o archivos antes de enviarlos y utilizar canales formales y seguros. 3) En el diseño de los sistemas, cuando se traten datos personales y exista un intercambio de información a través de servicios, deben estar configurados a través de un canal seguro, como por ejemplo TLS y seleccionar el cifrado más fuerte disponible para que el intercambio de información sea encriptado.

IV. RECOMENDACIONES PARA EL DEBIDO CUMPLIMIENTO POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO DE LAS DISPOSICIONES COMPRENDIDAS EN LA LEY N°19.628, EN RELACIÓN AL USO SEGURO DE HERRAMIENTAS TECNOLÓGICAS QUE PERMITEN EL TELETRABAJO Y EL TELEAPRENDIZAJE.

a) Finalmente, el Consejo para la Transparencia, ha advertido que en el contexto de la emergencia sanitaria ocasionada por el brote de COVID-19, diversos organismos públicos han adoptado soluciones tecnológicas que permiten a sus funcionarios desempeñar sus labores habituales bajo modalidades de trabajo a distancia y teletrabajo, tales como programas computacionales de sincronización y uso compartido de archivos institucionales, herramientas digitales de acceso remoto a escritorios, sistemas de almacenamiento en la nube, plataformas de videollamadas grupales y reuniones en línea, y otros programas computacionales de gestión de tareas. Asimismo, se han disponibilizado herramientas de teleaprendizaje, las que van dirigidas especialmente a niños, niñas y adolescentes.

b) A este respecto, suscita especial preocupación la eventual existencia de vulnerabilidades o brechas de ciberseguridad que podrían afectar la confidencialidad de la información de los usuarios de estas herramientas y de otros datos que se encuentren sujetos a deberes de reserva. Junto con ello, existe a su vez la posibilidad que estos sistemas lleven a cabo operaciones de tratamiento de información que resulten ser excesivas y no proporcionales en relación con los servicios y funcionalidades que prestan, en desmedro de la debida protección de los datos de carácter personal, y en algunos casos sensibles, cuando se trate por ejemplo de los datos de menores de edad.

c) El Consejo para la Transparencia hace hincapié en que el empleo de este tipo de herramientas no puede implicar una afectación de la privacidad, la intimidad o la protección de los datos personales de sus usuarios, en cuanto se trata de derechos fundamentales expresamente consagrados y asegurados en la Constitución Política.

d) En primer término, en cuanto a la decisión de utilizar una determinada herramienta informática que facilite el trabajo o aprendizaje no presencial o remoto, ésta **no puede circunscribirse únicamente a elementos relativos a su funcionalidad y eficiencia, debiendo prestarse especial atención a las garantías que ofrecen dichas herramientas en cuanto a la efectividad de las medidas de seguridad informática de que disponen y al adecuado tratamiento de los datos personales de sus usuarios**, los que en algunos casos serán incluso menores de edad.

En este sentido, el Consejo para la Transparencia recomienda que esta clase de decisiones esté **precedida por un análisis exhaustivo de las eventuales vulnerabilidades y riesgos de privacidad asociados a la solución tecnológica que se pretende implementar**, junto con una revisión detallada de las condiciones

contractuales, términos de uso y políticas de privacidad aplicables a dicha herramienta, respecto de los distintos dispositivos o sistemas operativos donde puede ser instalada y sus diversos formatos (sea software de escritorio, aplicación móvil o versión web).

e) Luego, en segundo lugar, se recomienda que las instituciones establezcan **políticas generales aplicables al uso de sistemas y programas informáticos en los contextos de trabajo remoto y teleaprendizaje**, asegurándose su observancia por parte de los funcionarios que se desempeñan bajo dichas modalidades. A este respecto, se deben abordar con especial atención aquellos aspectos vinculados a la seguridad de la información y la protección de los datos personales y sensibles de los propios usuarios y de los terceros.

f) En tercer término, **para la determinación de las medidas de seguridad aplicables,** se aconseja ponderar previamente la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados, con una mirada de capas o niveles de protección. Entre otros aspectos, se deben tener presente los riesgos de seguridad asociados al uso por parte de los funcionarios de sus dispositivos y redes personales para establecer conexiones remotas, en consideración a la posible ausencia de controles y salvaguardas similares a aquellos presentes en los equipos institucionales.

Por otra parte, resulta fundamental que **las instituciones establezcan protocolos que les permitan, en los contextos de trabajo y aprendizaje remoto, identificar y enfrentar incidentes que pueden afectar la seguridad de la información**, esto es, brechas que impliquen la filtración, pérdida o alteración accidental o ilícita de datos personales o reservados, o la comunicación o acceso no autorizados a dichos datos.

g) En cuarto lugar, **tratándose de datos cuyos titulares corresponden a menores de edad, deberán adoptarse los más altos estándares de seguridad en su procesamiento.** Lo anterior, en coherencia con lo afirmado por esta Corporación en diversas oportunidades en el sentido de señalar que se debe prestar especial atención y resguardo más intenso en las operaciones de tratamiento de datos de niños, niñas y adolescentes, ya que éstos pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de éstos. Este Consejo para la Transparencia reitera que los datos personales de menores de edad son, *per se*, datos personales sensibles y que, por lo tanto, deben ser especialmente protegidos.

h) En quinto lugar, este Consejo hace presente además que **corresponde a la institución usuaria verificar que la solución tecnológica asegure que el procesamiento de los datos recolectados o comunicados a través de dicha herramienta se ajustará en todo momento a la normativa vigente**, especialmente en lo que respecta a:

i) La licitud y proporcionalidad de los tratamientos de datos;

ii) La estricta observancia del principio de finalidad;
iii) El cumplimiento de los deberes de seguridad, confidencialidad y responsabilidad;
iv) La limitación de los plazos de conservación de los datos personales objeto de tratamiento; y,
v) La efectiva posibilidad que tienen los titulares de los datos de ejercer los derechos reconocidos en la ley N°19.628, en particular, los derechos de acceso, rectificación, cancelación, bloqueo y oposición.

i) En sexto lugar, tratándose de la **seguridad de estos sistemas**, deben preferirse soluciones tecnológicas confiables, que cuenten, al menos, con los siguientes elementos:

i) Dispongan de mecanismos de cifrado de extremo a extremo de la información que por dicha vía sus usuarios acceden y comparten;

ii) Ofrezcan garantías respecto de la seguridad de las credenciales de acceso, disponiendo, por ejemplo, de dobles factores de autenticación-, junto con proteger adecuadamente el acceso a la cámara web y micrófono de los equipos de sus usuarios, evitando de esta forma la filtración de información o el monitoreo de la actividad de los usuarios por terceros no autorizados;

iii) Permitan a la institución usuaria la trazabilidad de las actividades asociadas a la herramienta, entregándole los respectivos permisos de administrador. Esta evaluación resulta especialmente crítica respecto de aquellas plataformas que son utilizadas para acceder o transmitir categorías especiales de información, sometidas a deberes estrictos de confidencialidad.

j) En séptimo lugar, resulta necesario **mantener el software o aplicación en cuestión permanentemente actualizado**, con su última versión disponible, ejecutando siempre esta actualización directamente sobre el programa mismo y no a través de hipervínculos.

k) En octavo lugar, tratándose de las **plataformas de videollamadas grupales**, resulta especialmente relevante **evaluar los datos personales que esta clase de herramienta informática recolecta**, sea directamente (por ejemplo, al crear una cuenta de usuario) o a partir de su operación (esto es, la recopilación pasiva y automática de datos, vinculada al seguimiento de la actividad del usuario).

Específicamente, debe comprobarse que los datos recabados por el sistema no sean excesivos en relación con el servicio que presta, teniendo especialmente presentes los principios de proporcionalidad y de finalidad del tratamiento de datos personales. Así, corresponde constatar, por ejemplo, si la plataforma informa claramente y sin ambigüedades en sus políticas acerca de la posible comunicación de los datos recabados a terceros, para finalidades que no se condicen con la

prestación de los servicios que motivan el uso de dicho sistema o de alguna de sus funcionalidades.

A dicho respecto, es importante también considerar las siguientes recomendaciones para proteger la privacidad de los datos al momento de realizar la videollamada:

i) Seleccionar las opciones de privacidad básicas que vienen con las aplicaciones, por ejemplo, que la reunión sea privada y no pública.
ii) Permitir solo participantes registrados: la inscripción de los participantes permite tener un control de los asistentes.
iii) No entregar el control de la pantalla compartida: restringir que los participantes tomen control de la pantalla en un evento evitará que se compartan contenidos no deseado con el resto de los participantes.

l) Finalmente, **respecto a la recopilación pasiva de datos**, se aconseja verificar en los términos y condiciones de uso, así como en las opciones de configuración, el posible almacenamiento por parte de la plataforma tecnológica de la información o datos transmitidos y examinar los permisos o autorizaciones que, por defecto, solicita la herramienta para operar en un determinado dispositivo.

7. Asimismo, tenga presente que al disponibilizar información estadística sobre la pandemia, de carácter oficial, que permita facilitar el trabajo de investigación de laboratorios, centros médicos, de estudios y universidades, y, en general, de cualquier interesado en dicha información, se deberán siempre adoptar los mayores estándares de seguridad que garanticen que los datos en cuestión sean irreversiblemente anonimizados, de forma que no puedan luego ser asociados a un titular identificado o identificable.
8. Por último, este Consejo reitera su voluntad de colaborar, en el marco de sus competencias legales, en los esfuerzos estatales desplegados para hacer frente a esta pandemia mundial que nos afecta y, en particular, para el adecuado tratamiento de los datos personales que supone su control y gestión.

Sin otro particular, saluda atentamente a usted,

REPUBLICA DE CHILE
Directora General
CONSEJO PARA LA TRANSPARENCIA

ANDREA RUIZ ROSAS