APRUEBA RÉGIMEN DE RESPONSABILIDADES INDIVIDUALES PARA SATISFACER LOS REQUISITOS, NORMATIVAS Y LEYES RELATIVOS A LA IMPLEMENTACIÓN Y APLICACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN A LA JUNAEB.

JUNAEB 21 FEB 2017 OFICINA DE PARTES

RESOLUCIÓN EXENTA N° 2366

SANTIAGO, 7 de noviembre de 2016.

VISTO:

Lo dispuesto en la Ley Nº 15.720, que crea la Junta Nacional de Auxilio Escolar y Becas; en la Ley Nº 18.575 sobre Bases Generales de la Administración del Estado; en la Ley N° 19.880 de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en la Ley N° 18.834 sobre Estatuto Administrativo; en el Decreto Supremo de Educación Nº 5.311 de 1968 que Aprueba el Reglamento General de JUNAEB; en el Decreto Ley de Educación Nº 180, de 1973 que Reorganiza la Junta Nacional de Auxilio Escolar y Becas; en la Ley N° 17.336 de 1970 sobre Propiedad Intelectual; en la Ley N° 19.223 de 1993 sobre Delitos Informáticos; en el Instructivo presidencial N° 05 de 2001 que define el concepto de Gobierno Electrónico; en la Ley N° 19.628 de 1999 sobre Protección de la Vida Privada y Datos Personales; en la Ley N°19.799 de 2002 sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma; en el Decreto Supremo del Ministerio de Economía, Fomento y Turismo N° 181 de 2002 sobre Reglamento de la Ley N° 19.799; Instructivo Presidencial N° 06 de 2002 que imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la Administración del Estado; en el Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 77 de 2004, relativo a la Norma técnica sobre eficiencia de las comunicaciones electrónicas entre los Órganos de la Administración del Estado y entre éstos y los ciudadanos; en el Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 81 de 2004, relativo a la Norma técnica para los Órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos; en la Ley N° 19.927 de 2004 sobre delitos de pornografía infantil; Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 83 de 2005, relativo a la Norma Técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 93 de 2006, relativo a Norma técnica para minimizar la recepción de

mensajes electrónicos masivos no deseados e las casillas electrónicas de los órganos de la administración del Estado; Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 100 de 2006, sobre Norma Técnica para el desarrollo de los sitios web de los Órganos de la Administración del Estado y de sus funcionarios; Instructivo Presidencial N° 8 de 2006 que imparte instrucciones sobre transparencia activa y publicidad de la información de la Administración del Estado; Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 158 de 2007, que modifica el Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 81; Circular del Ministerio Secretaría General de la Presidencia N° 3 de 2007 que detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del Instructivo Presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado; Ley N° 20.285 de 2008 sobre Acceso a la Información Pública; Instrucción General del Consejo para la Transparencia N° 3 de 2009, sobre índice de actos o documentos calificados como secretos o reservados; Norma Chilena NCH-SO 27.001 Of2013 del Instituto Nacional de Normalización, sobre Sistemas de Seguridad de la Información; Decreto Supremo del Ministerio Economía, Fomento y Turismo N° 14 de 2014, que modifica el Decreto del Ministerio Economía, Fomento y Turismo N° 181; en el decreto supremo del Ministerio de Educación N° 292 de 2 de noviembre de 2016, que nombra a don Cristóbal Acevedo Ferrer como como Secretario General de la Junta Nacional de Auxilio Escolar; y en la Resolución N° 1600 del año 2008 de Contraloría General de la Republica, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, en virtud del Decreto Exento N° 231 de 24 de julio de 2016 del Ministerio de Hacienda, se aprueba el Programa Marco de los Programas de Mejoramiento de la Gestión (PMG) para el año 2016; el cual consta de dos áreas prioritarias y cuatro sistemas de gestión con sus respectivos objetivos, debiendo los servicios formular compromisos en uno o más sistemas de gestión, dependiendo del grado de desarrollo alcanzado a la fecha de la formulación.

2. Que, en lo que respecta a la Junta Nacional de Auxilio Escolar y Becas, uno de los Programas de Mejoramiento de la Gestión dice relación con el Sistema de *Seguridad de la Información,* correspondiente al área de Calidad de Servicio y que tiene por objetivo de gestión "*Gestionar los riesgos de seguridad de la información de los activos que soportan los procesos de provisión de bienes y servicios, mediante la aplicación de controles basados en la Norma NCH-ISO 27001*".

3. Que, la Norma NCHI-ISO 27001 de 2013 sobre Sistemas de Seguridad de la Información, dispone en el punto 5.3 denominado "*Roles organizacionales, responsabilidades y autoridades*" que "*la alta dirección debe asignar la responsabilidad y autoridad para: a) asegurar que el sistema de gestión de la seguridad de la información cumple con los requisitos de esta norma ; y b) informar a la alta dirección sobre el*

desempeño del sistema de gestión de la seguridad de la información."

4. Que, el punto 6.2 denominado "*Objetivos de seguridad de la información y planificación para lograrlos"* de la referida norma NCHI-ISO 27001 de 2013, prescribe en la letra h) como uno de los objetivos a establecer en la implementación del sistema de seguridad de la información, por parte del servicio que se trate, la determinación de un responsable.

5. Que, a mayor abundamiento, el Anexo A (normativo) de la norma NCHI-ISO 27001 de 2013, denominado "*Objetivos de control de referencia y controles*", establece como control, a propósito de los Roles y responsabilidades de la seguridad de la información que *"todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas".*

RESUELVO:

ARTÍCULO PRIMERO: APRUÉBESE el presente Régimen de Responsabilidades para la implementación y aplicación del Sistema de Seguridad de la Información, respecto de la Junta Nacional de Auxilio Escolar y Becas:

RESPONSABILIDADES INDIVIDUALES PARA SATISFACER LOS REQUISITOS, NORMATIVAS Y LEYES

Nombre o número del requisito, normativa o ley	Responsable
Norma ISO 27001:2013; sobre Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación**: Encargado/a de Seguridad de la Información **Aplicación**: Es responsabilidad de todo el personal de JUNAEB (interno, externo) el dar cumplimiento a esta normativa.
Ley N°19.799 de 2002; sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha firma.	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación:** Departamento Jurídico. **Aplicación**: Jefaturas de Departamentos y Unidades.
Decreto Supremo del Ministerio de Economía,	**Asegurar cumplimiento norma**: Jefe Superior del Servicio.

Fomento y Turismo N° 181 de 2002; sobre Reglamento de la Ley N° 19.799.	**Asesoría y consejo en implementación y aplicación:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Jefaturas de Departamentos y Unidades.
Instructivo Presidencial N° 05 de 2001; que define el concepto de Gobierno Electrónico	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación:** Departamento Jurídico **Aplicación**: Jefaturas de Departamentos y Unidades, funcionarios.
Instructivo Presidencial N° 06 de 2002; que imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la Administración del Estado	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Jefaturas de Departamentos y Unidades.
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 77 de 2004; relativo a la Norma técnica sobre eficiencia de las comunicaciones electrónicas entre los Órganos de la Administración del Estado y entre éstos y los ciudadanos.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Jefaturas de Departamentos y Unidades, funcionarios.
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 81 de 2004; relativo a la Norma técnica para los Órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación:** Departamento Jurídico. **Aplicación**: Jefe Departamento de Informática.
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 158 de	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio.

2007; que modifica el Decreto Supremo N° 81 de 2004.	**Asesoría y consejo en implementación y aplicación:** Departamento Jurídico. **Aplicación**: Jefe Departamento de Informática
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 83 de 2005; relativo a la Norma Técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Jefaturas de Departamentos y Unidades, funcionarios.
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 93 de 2006; relativo a Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados e las casillas electrónicas de los órganos de la administración del Estado.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico. **Aplicación**: Jefatura Departamento de Informática.
Decreto Supremo del Ministerio Secretaría General de la Presidencia N° 100 de 2006; sobre Norma Técnica para el desarrollo de los sitios web de los Órganos de la Administración del Estado y de sus funcionarios.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Jefatura Departamento de Informática.
Ley N° 20.285 de 2008; sobre Acceso a la Información Pública.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico y Departamento de Informática. **Aplicación**: Encargada Oficina de Atención Ciudadana y Unidades, funcionarios.
Instrucción Gral. N°3 del Consejo para la Transparencia de 2009; sobre índice de actos o	

documentos calificados como secretos o reservados.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico. **Aplicación**: Encargada Unidad de Gestión Documental
Ley N° 19.628 de 1999; sobre Protección de la Vida Privada y Datos Personales.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y cumplimiento:** Departamento Jurídico y Encargado del Registro o Banco de Datos de Carácter Personal de JUNAEB. **Aplicación:** Jefaturas de Departamentos y Unidades, funcionarios
Decreto Supremo N° 14 del Ministerio de Economía, Fomento y Turismo 2014; que modifica el Decreto N° 181 sobre Reglamento de la Ley N° 19.799.	Observancia corresponde al Ministerio de Secretaría General de la Presidencia
Instructivo Presidencial N° 8 de 2006; que imparte instrucciones sobre transparencia activa y publicidad de la información de la Administración del Estado.	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en cumplimiento e implementación:** Departamento Jurídico, Encargado del Registro o Banco de Datos de Carácter Personal de JUNAEB. **Aplicación:** Encargado/a Oficina de Atención Ciudadana, Encargado/a Unidad de Gestión Documental.
Circular del Ministerio Secretaría General de la Presidencia N° 3 de 2007; que detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del Instructivo Presidencial sobre transparencia activa y publicidad de la	**Asegurar cumplimiento de la norma**: Jefe Superior del Servicio. **Asesoría y consejo en cumplimiento e implementación:** Departamento Jurídico y Departamento de Informática. **Aplicación:** Encargado/a Oficina de Atención Ciudadana, Encargado/a Unidad de Gestión Documental.

información de la Administración del Estado.	
Ley N° 17.336 de 1970; sobre Propiedad Intelectual.	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación**: Departamento Jurídico JUNAEB **Aplicación**: Es responsabilidad de todo el personal de JUNAEB (interno, externo) el dar cumplimiento a esta normativa.
Ley Nº 19.223 de 1993; sobre Delitos Informáticos.	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación**: Departamento Jurídico y Departamento de Informática. **Aplicación**: Es responsabilidad de todo el personal de JUNAEB (interno, externo) el dar cumplimiento a esta normativa.
Ley N° 19.927 de 2004; sobre Delitos de pornografía infantil.	**Asegurar cumplimiento norma**: Jefe Superior del Servicio. **Asesoría y consejo en implementación y aplicación**: Departamento Jurídico y Departamento de Gestión de Personas. **Aplicación**: Es responsabilidad de todo el personal de JUNAEB (interno, externo) el dar cumplimiento a esta normativa.

ARTÍCULO SEGUNDO: ARCHÍVESE copia del presente acto administrativo.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN EL BANNER DE GOBIERNO TRANSPARENTE.

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS
SECRETARIO GENERAL

CRISTOBAL ACEVEDO FERRER

SECRETARIO GENERAL

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

RDM/MVJ/CES
DISTRIBUCIÓN

1. Gabinete Dirección Nacional
2. Departamento Jurídico
3. Departamento de Planificación y Estudios
4. Oficina de Partes.

NORMATIVA APLICABLE A LA SEGURIDAD DE LA INFORMACION

Elaborador por:	Depto. de Planificación, Control de Gestión y Estudios

1. CONTEXTO

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales, por ello se hace necesario describirlos y dejarlos documentados.

2. OBJETIVO

El presente documento tiene por finalidad identificar la legislación vigente y los requisitos contractuales pertinentes al Sistema de Seguridad de la Información de JUNAEB, describiendo a modo resumido sus implicancias y detalles más relevantes. De esta manera, se pueda dar cumplimiento a sus disposiciones y evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de infracciones u omisiones.

3. ALCANCE

Este procedimiento puede ser implementado a nivel nacional, y considera al Sistema de Seguridad de la Información que JUNAEB ha implementado en su servicio.

INDICE

21. **Norma Chilena NCh-ISO 27.001:2013**

Esta normativa corresponde a un modelo que busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SSI). En ella se encuentra la estructura necesaria, para organizaciones públicas y privadas, que permiten proteger la integridad, disponibilidad y confidencialidad de los activos de información, es decir, de la información misma como de los medios y la infraestructura que la soporta.

La NCH-ISO 27.001 establece una serie de controles que permiten mitigar los riesgos que puedan afectar a los activos de información de la organización. Estos controles están asociados a diversos dominios que incluyen la gestión y protección de recursos humanos, activos tecnológicos, soportes e infraestructura, seguridad, ambiente, normativa y continuidad del negocio, entre otros.

La normativa entonces, específica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones. El SSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a los usuarios internos y externos de la organización.

22. **Ley N° 19.799 de 2002, del Ministerio de Economía, sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.**

Este texto legal regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que deben someterse quienes prestan dicho servicio, con el objeto de garantizar la seguridad en su uso.

Esta Ley establece la firma electrónica, definiéndola como *"cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor"*[1]. Para ello el autor o titular, deberá utilizar bajo su exclusivo control el certificado de firma electrónica, cumpliendo con los requisitos que le exige la legislación y actuando en base a los derechos que ésta le concede.

Asimismo, la normativa, explicita la existencia de la firma electrónica avanzada, la cual es *"aquella certificada por prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría"*[2]. Esta firma, permite que electrónicamente se autentique la identidad del solicitante, se asegure la integridad de los documentos firmados y se evite la repudiación de los mismos, es por ello que los documentos que tengan calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

Según la normativa en su Artículo N° 3, *"los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escritos y en soporte de papel"*[3], es decir, la firma electrónica será considerada como firma manuscrita para todos los efectos legales, a excepción de

[1] Ministerio de Hacienda. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640

[2] Ministerio de Hacienda. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640

[3] Ministerio de Economía. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640

aquellos actos o contratos que la misma Ley establece (cuando la ley exige solemnidad que sea susceptible de cumplirse mediante documento electrónico, aquellos en que se requiera concurrencia personal y aquellos actos relativos al derecho de familia).

El Título II de la Ley N° 19.799, norma el uso de firmas electrónicas por los órganos del Estado y expone, en el Artículo N° 6, que éstos *"podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica"*[4]

El Artículo N° 8 expone que tal y como los órganos del Estado pueden relacionarse vía documentos y firma electrónica con organismos, las personas también podrán hacerlo con los *"órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos"*[5].

Finalmente, y en base a los principios de transparencia e igualdad de oportunidades, los órganos del Estado deberán evitar, *"hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se causen discriminaciones arbitrarias"*[6]

23. **Decreto Supremo N° 181 de 2002, del Ministerio de Economía, sobre reglamento de la Ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.**

    Este reglamento establece la normativa asociada a los documentos electrónicos, firma electrónica y a la certificación de la misma, *"por las personas naturales y jurídica de derecho privado y la administración del Estado"*[7]

    Este decreto establece las orientaciones que norman a los prestadores de servicios y la acreditación de los mismos, aunque pone mayor énfasis en la descripción detallada de los documentos electrónicos y su validación cuando son emitidos por órganos del Estado.

24. **Instructivo Presidencial N° 05 del 2001, que define concepto de Gobierno Electrónico.** Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.

25. **Instructivo Presidencial N° 06 del 2004, que imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado,** para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.

[4] Ministerio de Economía. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640
[5] Ministerio de Economía. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640
[6] Ministerio de Economía. Ley 19.799 http://www.leychile.cl/Navegar?idNorma=196640
[7] Ministerio de Economía. Decreto Supremo 181. http://www.leychile.cl/Navegar?idNorma=201668

26. **Decreto Supremo N° 77 del 2004, del Ministerio Secretaría General de la Presidencia, sobre Norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado y entre éstos y los ciudadanos.**

Esta norma regula *"las comunicaciones que se realizan por medios electrónicos y que tengan lugar entre los órganos de la Administración del Estado y las de éstos con las personas en todos aquellos ámbitos no regulados por otras normas legales, reglamentarias o administrativas específicas"*[8]

Asimismo, en el artículo N° 2, se hace explícito que las acciones asociadas a las comunicaciones deben estar reguladas y bajo el marco de los principios de *"legalidad, efectividad, eficiencia, publicidad y transparencia",* por lo que aparte de cumplir con la legalidad, cualquier tipo de transmisión o recepción de comunicaciones entre los órganos de la Administración del Estado o entre éstos y cualquier persona, deben cumplir con los siguientes requisitos (artículo N° 3):

- Asegurar la disponibilidad y acceso para uso posterior.
- Asegurar la compatibilidad de los sistemas utilizados por el emisor y el destinatario de modo que, permitan las comunicaciones entre ambos, incluyendo la utilización de código y formatos o diseños de registro establecidos por los órganos de la Administración del Estado.
- Contar con medidas de seguridad que permitan evitar la intercepción, obtención, alteración y otras formas de acceso no autorizado a las comunicaciones electrónicas, de conformidad con las normas técnicas generadas por el Comité de Normas para el Documento Electrónico sobre seguridad y confidencialidad del documento electrónico.
- Asegurar que los órganos de la Administración del Estado designen una o más direcciones electrónicas, que sean consideradas aptas para la recepción de dichas comunicaciones. Estas deberán encontrarse debidamente puestas a disposición o consultables por cualquier interesado.

Además de lo anterior, el Decreto Supremo N° 77 aclara que los organismos del Estado no sólo deben tener un medio de transmisión para la comunicación, sino que éste debe estar en un formato estándar u otros, siempre y cuando se publique su tipo y la aplicación necesaria para acceder al contenido, la cual debe ser de distribución y uso gratuito y accesible desde el sitio web correspondiente (Artículo N° 4).

Cualquier tipo de comunicación electrónica entre el Estado y una persona natural o jurídica, debe estar bien estructurada por lo que, según el Artículo N° 5, "*sólo se considerarán aquellas comunicaciones electrónicas que efectivamente contesta preguntan consistentes y fundadas, que digan relación con materias propias de la competencia de cada servicio público y que, en consecuencia, requieran de un pronunciamiento formal*" y, además, la persona natural o jurídica deberá individualizar con precisión la dirección de correo electrónico y otro medio autorizados, a la que cual desea se le avise la disponibilidad de respuesta.

Como medio de respaldo, "*deberá quedar constancia de la transmisión y recepción de las comunicaciones efectuadas por medios electrónicos e identificarse el remitente, destinatario, fecha y hora de la mismas*". No obstante, para asegurar la constancia de la comunicación, los órganos de la Administración del Estado deberán "*conservar los registros de estas comunicaciones por un periodo de tiempo que no podrá ser inferior a 6 años*" (artículo N° 6) y adjuntar los antecedentes que permitan la búsqueda y recuperación de la documentación almacenada por el tiempo señalado (artículo N° 7).

Además de lo señalado con anterioridad, el texto legal expone que las comunicaciones efectuadas por medios electrónicos deberán asegurar la integridad y confidencialidad de la información que almacenan, por lo que, cuando corresponda, "*se podrá utilizar un mecanismo de autentificación o de control de acceso a las direcciones electrónicas que contengan las respuestas que dé la Administración del Estado*" (artículo N° 11).

[8] Ministerio Secretaría General de la Presidencia. Decreto Supremo N° 77. http://www.leychile.cl/Navegar?idNorma=233912

27. **Decreto Supremo N° 81 de 2004, del Ministerio Secretaría General de la Presidencia, sobre norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos.**

Esta norma técnica, establece las "*características mínimas obligatorias de la interoperabilidad que deben cumplir los documentos electrónicos en su generación, envío, recepción, procesamiento y almacenamiento, tanto en los órganos de la Administración del Estado, como en las relaciones de la ciudadanía y el sector privado con dichos órganos, y las demás cuya aplicación se recomienda*"[9] (Artículo N° 1). Lo anterior con la finalidad de asegurar la interoperabilidad en la comunicación de datos e información entre diferentes organismos que utilicen documentos electrónicos.

En relación a lo anterior, el artículo mencionado expone que los órganos de la Administración del Estado deben estar provistos de un mecanismo que *"permita a los diferentes organismos que utilicen documentos electrónicos, encontrarse, convenir en comunicarse, desarrollar servicios, contar con estándares de repositorios para registro y consulta por parte de los diferentes órganos de la administración del Estado, de la información que cada uno de ellos mantiene y refleja"*[10].

Además, la normativa establece las características asociadas al documento electrónico y al registro (de almacenamiento) que permitirá darle trazabilidad a la petición y respuesta de información. Asimismo, expone los requisitos técnicos asociados al documento, de la firma electrónica y los soportes tecnológicos y digitales que deben sustentar el proceso de operatividad de información entre los organismos de la Administración del Estado.

28. **Decreto Supremo N° 158 de 2007, del Ministerio Secretaría General de la Presidencia, que modifica Decreto Supremo N° 81 sobre norma técnica para la interoperabilidad de documentos electrónicos.**

El Decreto Supremo 158 de 2007, modifica el artículo primero del Decreto Supremo 81 de 2004, en donde precisa que la interoperabilidad de los documentos electrónicos es para los "órganos de la Administración Central del Estado, lo que comprende los *"servicios públicos descentralizados, pero no incluye a las municipalidades, a las empresas del Estado ni a las Universidades públicas"*[16].

29. **Decreto Supremo N° 83 de 2005, del Ministerio Secretaría General de la Presidencia, sobre norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.**

El Decreto Supremo 83 "*establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines*"[17] (Artículo N° 1), esto con la finalidad de garantizar estándares de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico, facilitar la relación electrónica entre los órganos del Estado y resguardar el uso

[9] Ministerio Secretaría General de la Presidencia. Decreto Supremo 81. http://www.leychile.cl/Navegar?idNorma=233913
[10] Ministerio Secretaría General de la Presidencia. Decreto Supremo 81. http://www.leychile.cl/Navegar?idNorma=233913 [16] Ministerio Secretaría General de la Presidencia. Decreto Supremo 158. http://ssi.pmg.gov.cl/filesapp/DTO-158_18-MAY2007.pdf

del documento electrónico poniendo énfasis en la confiabilidad, seguridad y en el pleno respeto de las normativas existentes en esta materia.

Asimismo el Artículo N° 2, expone que las disposiciones de la norma técnica *"se aplicarán a los documentos electrónicos que se generen, intercambien, transporten y almacenen en o entre los* [17]*diferentes organismos de la Administración del Estados y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos"*[11]
Para los efectos de la mencionada norma, como también para las normas descritas anteriormente, los *"documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella"*[19] (Artículo N° 3)

El Decreto Supremo 83, es la norma que establece en la normativa chilena la ISO 27.001 sobre la Gestión de Seguridad de la Información por lo que se puede encontrar, a partir del Título III, una descripción detallada sobre los requisitos de seguridad que una institución debe implementar para resguardar la información con la que trabaja. Esta seguridad, según el Artículo N° 6, *"se logra garantizando los siguientes atributos:*

a) Confidencialidad
b) Integridad
c) Factibilidad de autenticación y,
d) Disponibilidad"[20]

Con el fin de garantizar los atributos antes mencionados, los órganos de la Administración del Estado sujetas a esta normativa, deben realizar una serie de acciones que permitan cumplir con el resguardo al que se hace mención. Estas acciones deben apuntar a:

a) Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento; b) Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;
c) Implementar los procesos y procedimientos señalados precedentemente;
d) Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad;
e) Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas;
f) Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las letras anteriores.

Las acciones que los órganos de la Administración del Estado deben emprender, tienen que estar orientadas a buscar la seguridad de los activos de información y, para ello, la normativa presenta una serie de controles que contemplan diferentes brechas que pueden generar amenazas para los activos, considerando desde los documentos en papel como los equipos tecnológicos. Estos controles deben implementarse de forma paulatina, comenzando con los niveles mínimos de seguridad exigidos por la norma, hasta llegar a un nivel avanzado que permita el reguardo total de la información de los órganos del Estado (Artículos N° 9 y 10).

[11] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.
[19] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.

Los controles mencionados con anterioridad, responden a Dominios que definen ciertos ámbitos de acción que fortalecen las medidas de seguridad para los activos de información que poseen las organizaciones del Estado. Para ello definir las acciones que aplican a cada organismo es de suma importancia y es por ello, que se exponen a continuación los dominios del Decreto Supremo N° 83 y la NCh 27.001: [20]

a) Política de Seguridad: Según el Artículo N° 11, en los órganos de la Administración del Estado debe *"establecerse una política que fije las directrices generales que orienten en materia de seguridad dentro de la institución"*[12]. En ésta deben incluirse los siguientes lineamientos: i) Definición de seguridad del documentos electrónicos, objetivos generales, alcance e importante; ii) Difusión de los contenidos al interior de la organización; y iii) reevaluación de forma periódica, a lo menos cada 3 años.
b) Seguridad Organizacional: *"En cada organismo regido por esta norma, deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos"*[13] (Artículo N°12). Asimismo, se recomienda formar un Comité de Seguridad de la Información, el cual tome las decisiones referidas a la implementación de los controles y el monitoreo de las acciones.
c) Clasificación, Control y Etiquetado de Bienes: La normativa expone que *"los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección"*[23]. La idea de clasificar los activos de información no sólo es dar cumplimiento a la normativa, sino que definir cuál es la importancia de éste dentro del proceso y quién es su responsable (Artículos 13 y 14).

   Asimismo, se debe proponer y estipular los procedimientos de manipulación requeridos para cubrir las necesidades de seguridad de los documentos electrónicos, es decir, sobre el i) copiado, ii) almacenamiento, iii) transmisión por correo electrónico y sistemas protocolarizados de transmisión de datos digitales y, iv) la destrucción de los documentos (Artículo N° 15).

   En caso de existir documentación confidencial, reservada o clasificada como secreto, deberá etiquetarse de forma apropiada que identifique al documento y/o activo tecnológico.
d) Seguridad física y del ambiente: El Artículo N° 17 del texto legal, expone que los equipos *"deberán protegerse de las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables"*[24], además de robos, acceso no autorizado a las áreas de trabajo y procesamiento, incendios, inundaciones, entre otras.

   Como medida de la dirección de la institución, *"cada órgano deberá impartir y publicitar instrucciones relativas a los siguientes aspectos: i) Consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos, ii) Condiciones climatológicas y ambientales que pueden afectar sistemas informáticos o entornos cercanos y, iii) Promoción de una práctica de escritorio limpio"*[25] (Artículo N° 18)
e) Seguridad del Personal: Parte importante de la seguridad a la que se refiere esta ley, son los resguardos que deben existir para quienes manipulan la información y los medios que la soportan, por lo que la normativa pone énfasis en los siguientes aspectos: *"i) Uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en*

[12] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598
[13] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598
[23] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598
[24] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. [26][25] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.

el computar; ii) Uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota y otros; iii) Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos; iv) Procedimientos para reportar incidentes de seguridad"[26].

Además de lo anterior y como parte importante de la seguridad de la información de cualquier organización, es definir bien las responsabilidades asociadas a la manipulación de documentos por lo que éstas deben estar *"explicitadas en la etapa de selección e incluirse expresamente en los decretos o resoluciones de nombramiento o en las contrataciones respectivas"*[14] (Artículo N° 21).

f) Gestión de las operaciones y comunicaciones: Este dominio está enfocado en las condiciones de seguridad que deben existir para proteger la gestión, la operatividad y las comunicaciones de la institución. Para ello, en el Artículo 22, se expone que deben explicitarse y difundirse los siguientes antecedentes e información: *"i) Los contactos de apoyo ante dificultados técnicas u operacionales inesperadas de sistemas informáticos; ii) Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado; iii) Las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de comunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar"*[28].
Como medio de seguridad paralelo a los mencionados con anterioridad, la normativa exige la realización de a lo menos un respaldo mensual de los computadores personales de institución. Para cumplir con los respaldos se de disponer con la infraestructura adecuada para su realización y almacenamiento, además del debido con el nivel apropiado de protección física de los medios.
Finalmente, y sumando a los controles establecidos por la normativa en este dominio, los órganos del Estado deben contar con instrucciones respecto al uso seguro del correo electrónico, dejando en claro la vulnerabilidad en el envío de documentos electrónicos y la administración de password y contraseñas.

g) Control de Acceso: Este dominio es establecido como una forma de identificar de manera formal y obligatoria a los usuarios que manejan la información. Para ello se debe ocupar identificadores válidos que permitan acceder a los sistemas de forma segura pero, a su vez, que sean confidenciales por lo que cada usuario debe tener cuidado de no exponer su información dejando por escrito sus passwords y/o contraseñas (Artículo N° 28)
La emisión y administración de las contraseñas debe estar normada por un procedimiento que especifique la forma segura de definir las contraseñas, recomendando número de caracteres, tiempo para su modificación, forma de utilización, entre otros. (Artículo N° 28). Además, como forma de mantener la conectividad pero a su vez la seguridad, la normativa expone que para ciertos usuarios, se *"deberá entregar identificadores temporales de una manera segura. Específicamente, se deberá evitar el uso de terceras partes o mensajes de correo electrónico no protegido (texto en claro) para comunicar el identificador"*[15] (Artículo N° 29). Asimismo en caso de que un usuario necesite hacer uso de varios sistemas o plataformas, se deberá entregar acceso a cada uno de ella de forma independiente *"para reducir el acceso no autorizado a documentos electrónicos o sistemas informáticos, se deberá promover buenas prácticas, como las de pantalla limpia"*[30] (Artículo N° 31)
Finalmente, los organismos de la Administración del Estado deberán *"controlar el acceso a los servicios de red internos y externos mediante el uso de identificadores o certificados digitales"* tales como las conexiones remotas y aquellas aplicaciones que restringen el acceso desde dentro como desde fuera de la institución (Artículo N° 32 y 33)

[14] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598 [28] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.

[15] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.

[30] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83.

h) Desarrollo y Mantenimiento de Sistemas: Para aquellos organismos que requieran precaver que la seguridad esté incorporada en los sistemas en la etapa de diseño, se entenderán como organismos complejos y para tal efecto, deberán adoptar las indicaciones que se estimen por la propia institución para la protección y seguridad de los datos e información que pudiesen contenerse en los sistemas de información.

i) Gestión de la Continuidad del Negocio: *"El encargado de seguridad deberá formular un Plan de Contingencia para asegurar la continuidad de las operaciones críticas para la institución. Este plan deber, como mínimo, disponer la efectiva gestión de las relaciones públicas, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridades directivas, etc., y mecanismos eficaces para convocar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados"*[16] (Artículo N° 35)

Así como se describe anteriormente, la normativa expone y exige la aplicación de los estándares mínimos de seguridad para los activos de información de la Administración del Estado. Pero para garantizar la seguridad de los documentos electrónicos, el Decreto Supremo presenta una segunda etapa o nivel avanzado de aplicación en donde los diferentes servicios *"deberán desarrollar las políticas, procedimientos, acciones y medidas tendientes a la obtención del nivel avanzado de seguridad de los documentos electrónicos"*[32]. (Artículo N° 36). El desarrollo de políticas, procedimiento y otras acciones deberán transmitir el cumplimiento de las exigencias de seguridad y, por lo tanto, deberán ser consecuentes con todas las acciones emprendidas en el nivel básico descrito con anterioridad.

30. **Decreto Supremo N° 93 de 2006, del Ministerio Secretaría General de la Presidencia; sobre norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado.**

Con el objetivo de reducir el espacio de almacenamiento de los correos electrónicos y reducir las posibilidades de una infección por códigos maliciosos, spam y otros archivos que puedan afectar los archivos digitales, la presente norma *"establece las condiciones mínimas que deben cumplir los órganos de la Administración del Estado para el procesamiento y manejo de los mensajes electrónicos recibidos en sus infraestructuras de comunicaciones, y las demás cuya aplicación se recomienda"*[33] (Artículo N° 1). Estas condiciones mínimas tiene por *"finalidad minimizar, a través del establecimiento e implementación de medidas de seguridad adecuadas, los efectos perjudiciales de los mensajes electrónicos masivos no solicitados, enviados a las casillas electrónicos de los órganos de las Administración del Estado"*[34] para que así se garantice la integridad, permanencia, disponibilidad y acceso a la documentación electrónica y, a su vez, la confiabilidad de las comunicaciones electrónicas.

El Artículo N° 2 del Decreto Supremo 93, expone una serie de medidas que deben adoptar los órganos de la Administración del Estado para minimizar la recepción de mensajes recibidos en las infraestructuras electrónicas institucionales, las cuales se exponen a continuación:

---

[16] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598 [32] Ministerio Secretaría General de la Presidencia. Decreto Supremo 83. http://www.leychile.cl/Navegar?idNorma=234598 [33] Ministerio Secretaría General de la Presidencia. Decreto Supremo 93. http://www.guiadigital.gob.cl/sites/default/files/ds_93_2006.pdf [34] Ministerio Secretaría General de la Presidencia. Decreto Supremo 93. http://www.guiadigital.gob.cl/sites/default/files/ds_93_2006.pdf

a) Identificar y evaluar los riesgos y costos asociados a la recepción de mensajes electrónicos masivos no deseados, esto es, que no digan relación con el ámbito de competencia del respectivo órgano de la Administración del Estado.
b) Desarrollar, documentar y difundir políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos y de los sistemas informáticos utilizados en su procesamiento.
c) Diseñar, documentar e implementar los procesos y procedimientos necesarios para poner en práctica las diferentes políticas diseñadas para cumplir con las disposiciones de la norma.
d) Monitorear el cumplimiento de los procedimientos establecidos y revisarlos, de manera de reducir los costos asociados a la recepción de mensajes electrónicos masivos no deseados que no guarden relación con el ámbito de competencia del Servicio de que se trate.
e) Capacitar a los usuarios para operar la infraestructura de comunicaciones de acuerdo con las exigencias establecidas.
f) Definir y documentar los roles y responsabilidad de las unidades organizacionales e individuos involucrados en cada uno de los aspectos mencionados en las letras anteriores.

Cualquiera sea la acción emprendida por los órganos de la Administración del Estado, es necesario que en la infraestructura de comunicaciones que se utilice cada uno de ellos, se instale(n) el o los *"sistemas informáticos adecuados para filtrar los mensajes electrónicos a que se refiere esta norma, entrantes a su servidor o servidores de correo"*[17] (Artículo N° 3) los cuales deben ser protegidos para evitar un uso erróneo o indebido que pudiera causar detrimento de sus rendimiento o incapacidad de uno por parte de los usuarios validados y autorizados para ello.

Una parte importante en el resguardo de la información digital que almacena y se trasmite vía correo electrónico es que, debido a que los órganos de la Administración del Estado deben utilizar servicios de acceso a Internet provistos por privados, se debe cuidar la seguridad de la información que fluye por los medios por lo que se deben considerar los siguientes puntos (Artículo N° 5)
a) Que se cautele la correcta instalación y funcionamiento de los servidores de correo electrónico de sus clientes, para evitar open relay.
b) Que se ofrezca un punto de contacto para comunicarse con el encargado de seguridad informática del órgano de la Administración del Estado respectivo.
c) Que se monitoree, al menos semanalmente, la red bajo su responsabilidad, debiendo alertar al encargado de seguridad informática de la red responsable para que solucione problemas, en su caso.
d) Que se pone a disposición de sus clientes, en sus respectivos sitios web, las condiciones particulares de uso del servicio de correo electrónico que presta.

Las casillas electrónicas de la institución del Estado no podrán ser difundidas a través de su sitio web, esto para mantener y minimizar las posibilidades de recepción masiva de correos electrónicos (Artículo N° 6) por lo que *"los sistemas de procesamiento de mensajes electrónicos que el órgano de la Administración el Estado ponga a disposición de sus usuarios deben entregar facilidades para su filtrado con una configuración que garantice un nivel de protección adecuado, con especial consideración respecto de la inviolabilidad de las comunicaciones electrónicas"*[36] (Artículo N° 7).

[17] Ministerio Secretaría General de la Presidencia. Decreto Supremo 93. http://www.guiadigital.gob.cl/sites/default/files/ds_93_2006.pdf [36]
Ministerio Secretaría General de la Presidencia. Decreto Supremo 93. http://www.guiadigital.gob.cl/sites/default/files/ds_93_2006.pdf

Finalmente, como forma de asegurar un adecuado funcionamiento de las herramientas de filtrados dispuestas por la institución, estas deberán mantener un constante monitoreo y mantenimiento al menos cada seis meses de modo que no sólo se minimicen los posibilidades de ocurrencia de contingencias vía correo electrónico sino que también, fortalecerán los sistemas y acentuarán el medio de comunicación usado por la ciudadanía para mantener el contacto con las órgano de la Administración del Estado.

31. **Decreto Supremo N° 100 de 2006, el Ministerio Secretaría General de la Presidencia, sobre norma técnica para el desarrollo de los sitios web de los órganos de la Administración del Estado y de sus funcionarios.**

Este texto legal establece las características mínimas obligatorias que deben cumplir los órganos de la Administración del Estado para el desarrollo de los sitios web de gobierno, exponiendo que éstos deben *"ser desarrollados de manera tal que garanticen la disponibilidad y la accesibilidad de la información, así como el debido resguardo a los derechos de los titulares de datos personales, y asegurando la interoperabilidad de contenidos, funciones y prestaciones ofrecidas por el respectivo órgano de la Administración del Estado, con prescindencia de las plataformas, hardware y software"*[18]
"Todo sitio web deberá hacer uso del dominio .gov.cl y .gob.cl, registrándolos previamente ante la División de Informática del Ministerio del Interior; y del icono identificatorio del gobierno, el cual será proporcionado por el Ministerio Secretaría General de Gobierno. De igual modo, los sitios web deberán registrar en sus servicios de nombres las tablas reversas de la o las direcciones IP asociadas a los dominios gov.cl y gob.cl correspondientes"[19] (Artículo N° 3)

El Artículo N° 4 de la normativa expone que cuando se desarrollen sitios web se debe velar por disponibilidad de la información que en esta se emita, esto con el fin de garantizar el acceso a los contenidos que cada uno de los órganos de la Administración del Estado ponga a disposición de sus usuarios teniendo siempre en consideración la buena administración que permitan la correcta conexión e indexación de contenidos a los sistemas de catalogación y búsqueda y la optimización del peso y la calidad de los contenidos.

Además de lo anterior, la normativa entrega una serie de recomendaciones con las que deben cumplir los sitios web de gobierno, entre las cuales están: ser HTML o XML v1.0; cumplir con estándares HTML 4.01 o XHTML 1.0 validados antes el W3C, utilizar HTML validado y las cascadas de estilos provistas por la W3C. (Artículo N° 5)

El responsable de sitio web o también nombrado administrador, deberá *"monitorear regularmente la actividad del mismo (…) deberá revisar periódicamente el log del servidor que aloja el respectivo sitio web, prestando atención a los códigos de error ya los elementos más visitados y (…) adoptar las medidas preventivas y correctivas oportunas, en aras de mejorar la calidad de las prestaciones e información que se brindan por su intermedio"*[20] (Artículo N° 6)

Para cumplir con mantener la disponibilidad de la información de los sitios web, los órganos de la Administración del Estado deberán tener y mantener un plan de contingencia que contemplará las medidas necesarias en caso de incidentes que dejen sin acceso o sin disponibilidad a la información a los usuarios. (Artículo N° 7)

[18] Ministerio Secretaría General de la Presidencia. Decreto Supremo 100. http://www.leychile.cl/Navegar?idNorma=252158
[19] Ministerio Secretaría General de la Presidencia. Decreto Supremo 100. http://www.leychile.cl/Navegar?idNorma=252158
[20] Ministerio Secretaría General de la Presidencia. Decreto Supremo 100. http://www.leychile.cl/Navegar?idNorma=252158

El Artículo N° 9 de la normativa hace referencia a la Política de Privacidad de los sitios web que deben adoptar los órganos de la Administración del Estado. En este apartado recomienda seguir con las siguientes menciones:

a) La individualización del órgano de la Administración del Estado es responsable del tratamiento de datos a que corresponde el sitio web, con precisión de quien le represente, su domicilio, dirección postal y correo electrónico.

b) Una declaración, en términos claros y precisos, respecto a si el órgano de la Administración del Estado trata datos personales desde su sitio web, indicado, según sea el caso: el nombre del banco de datos personales; el fundamento jurídico de su existencia, la finalidad del banco de datos; el o los tipos de datos almacenados en dicho banco, y una descripción de la categoría de personas que comprende. Todo ello conforme lo registrado en el Registro de Bases de Datos que mantiene el Servicio de Registro Civil e Identificación, hacia el cual deberá existir un enlace a efectos de ser consultado por los usuarios.

c) Una declaración en cuanto a las condiciones y garantía sobre confidencialidad del tratamiento de los datos personales, así como el hecho de transferir datos terceros o procesar datos a través de estos, los cuales individualizará suficientemente, en su caso.

d) La declaración expresa de los derechos de que dispone el usuario, en cuanto titular de datos personales, para su debido resguardo, así como de los medios que dispone el propio órgano de la Administración del Estado para garantizar el ejercicio de los mismos.

e) La indicación de una dirección electrónica de contacto, a efectos de que el usuario solicita y obtenga, por medios electrónicos, información acerca de qué datos personales se mantienen registrados. Esta dirección electrónica de contacto permitirá a los usuarios, en tanto titulares de datos personales, solicitar acceso a los datos que les conciernen, así como su modificación, eliminación, cancelación o bloqueo. Con todo, tratándose del ejercicio del derecho de acceso, la respuesta del órgano de la Administración del Estado se verificará por medios electrónicos si dispusiere de garantías suficientes respecto a la identidad de la persona solicitante. En caso contrario, pospondrá la respuesta comunicando al titular los datos de la disponibilidad de ésta para serle entregada personalmente.

Para un nivel más avanzado, los Artículos N° 10, 11, 12, 13 y 14 presenta una serie de condiciones que entregan más seguridad a las páginas web de gobierno, entre las cuales encontramos:

a) Diagramación con hojas de cascadas de estilo; separando el contenido, la estructura y la presentación de los primeros. Además se recomienda validar las plantillas de las mismas, a través de las herramientas provistas por W3C.
b) Los marcos o frames deben ofrecer información adecuada al usuario.
c) En caso de emplear archivos que requieran de programas visualizadores especiales o plug-ins para su revisión, se deberá poner dichos programas a disposición de los usuarios para ser bajados desde el propio sitio web.
d) Los sitios web deben ser accesibles con diferentes navegadores, debiendo al menos uno de ellos ser de distribución y uso gratuito, y estar disponible desde el propio sitio web.

32. **Ley N° 20.285 sobre Acceso a la Información Pública de 2008, del Ministerio Secretaría General de la Presidencia, que regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.**

Esta norma tiene como objetivo principal regular *"el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos*

para el ejercicio del derecho y para su ampara, y las excepciones a la publicidad de la información"[21] (Artículo N° 1).

Esta Ley tiene su base en el inciso 2° del Artículo N° 8 de la Constitución Política en donde se establece que *"son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamento y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquellos o de esto, cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional"*[22], por lo que su aplicación es obligatoria en ministerios, intendencias, gobernaciones, gobiernos regionales, municipalidades, Fuerzas Armadas, Orden y Seguridad Pública, y los órganos y servicios público creados para el cumplimiento de la función administrativa. Para el caso de la Contraloría General de la República, el Banco Central de Chile y las empresas públicas, éstas se ajustarán a las disposiciones que esta ley señale expresamente para cada una de ellas.

Los órganos de la Administración del Estado desarrollan la función pública, la cual debe ejercerse con *"transparencia, de modo que permita y promueva el conocimiento de los procedimientos, contenidos y decisiones que se adopten en ejercicio de ella"*[42] (Artículo N° 3), por lo que los funcionarios de los servicios público deberán dar estricto cumplimiento al principio de transparencia (Artículo N° 4) y a las disposiciones de esta normativa.

"El principio de transparencia de la función pública consiste en respectar y cautelar la publicidad de los actos, resoluciones, procedimientos y documentos de la Administración, así como la de sus fundamentos, y facilitar el acceso de cualquier persona a esa información, a través de los medios y procedimientos que al efectos establezca la ley"[23] (Artículo N° 4). Este principio se apoya en los siguientes principios que expone, además, la ley (Artículo N° 5 y 6):

a) Principio de la relevación: Presume relevante toda la información que posean los órganos de la Administración del Estado, cualquier sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento.
b) Principio de la Libertad de Información: Toda persona goza del derecho a acceder a la información que obre en poder de los órganos de la Administración del Estado, sólo con excepciones o limitaciones establecidas por leyes de quórum calificado.
c) Principio de Apertura o Transparencia: toda la información en poder de los órganos del Estado se presume pública, a menos que esté sujeta a las excepciones señaladas.
d) Principio de Máxima Divulgación: Los órganos del Estado deben proporcionar información en los términos más amplios posibles, excluyendo sólo aquello que esté sujeto a las excepciones constitucionales o legales.
d) Principio de Oportunidad: Los órganos del Estado deben proporcionar respuesta a las solicitudes de información dentro de los plazos legales, con la máxima celeridad posible y evitando todo tipo de trámites dilatorios.
e) Principio de Gratuidad: El acceso a la información de los órganos de la Administración del Estado es gratuito, sin perjuicio de lo establecido en esta ley.

[21] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública. http://www.leychile.cl/Navegar?idNorma=276363
[22] Constitución Política de Chile de 1980. http://www.oas.org/dil/esp/Constitucion_Chile.pdf [42] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública.
[23] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública.

f) Principio de la Divisibilidad: Sólo si un acto administrativo contiene información que puede ser contenida se le dará acceso a quien requiera de ella, en el caso contrario, debe denegarse en virtud de una causa legal.

g) Principio de Facilitación: Los órganos de la Administración del Estado deben facilitar el ejercicio del derecho, excluyendo exigencia o requisitos que puedan obstruirlo o impedirlo.

h) Principio de la No Discriminación: Los órganos de la Administración del Estado deberán entregar información a todas las personas que la soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivo para la solicitud.

i) Principio de Control: El derecho al acceso a la información será objeto de fiscalización permanente.

j) Principio de la Responsabilidad: Los órganos de la Administración del Estado concurrirán en responsabilidad cuando no se dé cumplimiento a las obligaciones expuestas en esta ley.

Además de lo anterior, la ley N° 20.285 expone que la información debe ser publicada de forma proactiva en la página web de los órganos de la Administración y, a este acto, se le denomina Transparencia Activa y quiere decir que los órganos de la Administración del Estado tienen el deber de mantener a disposición permanente del público, a través de sus sitios electrónicos, determinados antecedentes actualizados, al menos una vez al mes, entre los cuales están: i) estructura orgánica, ii) facultades, funciones y atribuciones de cada una de sus unidades u órganos internos, iii) normativa aplicable, iv) personal de planta, contrata y honorarios, con las respectivas remuneraciones; v) contrataciones para el suministro de bienes muebles, vi) trámites y requisitos que debe cumplir el interesado para tener acceso a los servicios que preste y/o bienes que entregue el respectivo órgano, vii) mecanismos de participación ciudadana y viii) información presupuestaria asignada y ejecutada, siempre y cuando no sea información confidencial o secreta (Artículo N° 7). En todo caso, deberán estar disponibles permanentemente, en sitios web, los actos y documentos que han sido objeto de publicación en el Diario Oficial y aquellos que digan relación con las funciones, competencias y responsabilidades de los órganos de la Administración del Estado.

Los antecedentes mencionados con anterioridad, es decir, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustentos o complemento directo y esencial, y los procedimientos que se utilicen para su dictación son públicos, salvo las excepciones que establece esta ley y las previstas en otras leyes de quórum calificado. Asimismo, se considera pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, a menos que esté sujeta a las excepciones señaladas.

En relación al acceso a esta información pública, el artículo N° 10 de la Ley expone que *"toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece la ley"*[24]. Este derecho comprende el acceso *"a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdo, así como toda información elaborada con presupuesto público, cualquiera sea el formato o soporte en que se contenga"*[25]

[24] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública. http://www.leychile.cl/Navegar?idNorma=276363

[25] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública. http://www.leychile.cl/Navegar?idNorma=276363

Si bien toda persona tiene derecho al acceso a la información emitida por los órganos de la Administración del Estado, existen ciertas condiciones que se deben cumplir, las cuales se mencionan a continuación:

a) Identificación del solicitante: El Artículo N° 12 expone que la solicitud de acceso a la información será formulada por escrito -OIRS/SIIAC- o por sitios electrónicos y deberá contener: i) nombre, apellidos y dirección del solicitante o de su apoderado, según sea el caso, ii) identificación clara de la información que se requiere, iii) firma del solicitante estampada por cualquier medio habilitado y iv) órganos administrativo al que se dirige, por lo que si no se cumple con estas condiciones, el órgano de la Administración del Estado al cual fue solicitada la información puede pedir al solicitante que, en un plazo de 5 días hábiles, realice de nuevo la solicitud cumpliendo con las características exigidas.

Ingresada la solicitud, los órganos tienen un plazo máximo de 20 días hábiles para dar respuesta al peticionario (Artículo N° 14). En caso que el órgano de la Administración requerido *"no sea competente para ocuparse de la solicitud de información o no posea los documentos solicitados, enviará de inmediato la solicitud a la autoridad que deba conocerla según el ordenamiento jurídico, en la medida que ésta sea posible de individualizar, informando de ello al peticionario. Cuando no sea posible individualizar al órgano competente o si la información solicitada pertenece a múltiples organismos, el órgano requerido comunicará dichas circunstancias al solicitante"*[26] (Artículo N° 13).

Asimismo, en caso de que la institución se negara a dar acceso a la información al solicitante, debe justificar con vía legal tal razón. En caso de que las justificaciones cumplieran con lo dispuesto en la normativa, se considerarán causales de reserva las cuales comprenden las siguientes situaciones (artículo N° 20 y 21):

a) Cuando su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente: i) si es desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales, ii) tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquellas sean públicos una vez que sea adoptadas, iii) tratándose de requerimiento de carácter genéricos, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus laborales habituales.

b) Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.

c) Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente si se refiere a la Defensa Nacional o la mantención del orden público o la seguridad pública.

d) Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.

e) Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos (artículo N° 22)

[26] Ministerio Secretaría General de la Presidencia. Ley 20.285 sobre Acceso a l Información Pública.

La institución, cumpliendo con los plazos establecidos para dar respuesta a la solicitud, deberá entregarla por el medio que el solicitante expresó y además, deberá registrarla con el fin de mantener un control sobre la información que se transmite desde y hacia la institución[27].

En caso de que el órgano de la Administración del Estado no dé respuesta a la solicitud del peticionario, éste deberá recurrir al Consejo de Transparencia en donde deberá generar una petición. El Consejo dará aviso al órgano en cuestión y al peticionario informando de cómo se llevará el proceso. Emitida la resolución del Consejo de la Transparencia y avisados a los participantes, el solicitante podrá poner un recurso ante la Corte de Apelaciones la cual regulará de acuerdo al procedimiento administrativo y judicial (artículos N° 24-30).

33. **Instrucción General N° 3, del Consejo para la Transparencia, que presenta Índice de Actos o Documentos calificados como secretos o reservados.** Considerando que la información elaborada, gestionados y otras emanadas de los órganos del Estado y en base a la ejecución del Presupuesto del Sector Público, es información pública. No obstante, existe información que es confidencial, en especial aquella que emana de los órganos de las FF.AA y aquella que pueda poner en peligro la seguridad nacional y la vida privada de las personas.

34. **Ley N° 19.628 de 1999, del Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada y datos personales.**

La ley N° 19.628 es aquella que norma el tratamiento de datos de carácter personal en registros o bancos de datos administrados por organismos públicos o por particulares, teniendo como premisa que *"toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico"*[48], por lo que se debe tener en consideración los derechos fundamentales de los titulares de los datos que están en tratamiento. [48]

Debido a que esta normativa tiene como objetivo proteger los datos privados de las personas, se definen a continuación los conceptos más importantes (artículo N° 2):

a) Almacenamiento de datos: conservación o custodia de datos en un registro o banco de datos.
b) Bloqueo de datos: suspensión temporal de cualquier operación de tratamiento de datos almacenados.
c) Comunicación o transmisión de datos: dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular.
d) Dato caduco: dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese forma expresa, por el cambio de los hechos o circunstancias que consigna.
e) Dato estadístico: dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
f) Datos de carácter personal o datos personales: información concerniente a personas naturales, identificadas o identificables.
g) Datos sensibles: datos personales que hacen referencia a características físicas o morales de las personas o a hechos o circunstancia de su vida privada o intimidad, tales como los hábitos

[27] Procedimiento Administrativo. Título II. Ley 19.880 de 2003, del Ministerio Secretaría General de la Presidencia, sobre los procedimientos administrativos que rigen a los actos de la administración del Estado.
http://www.leychile.cl/Navegar?idNorma=210676

personales, el origen racial, las ideología y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) Eliminación o cancelación de datos: destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
i) Fuentes accesibles al público: registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.
j) Modificación de datos: cambio en el contenido de los datos almacenados en registros o bancos de datos.
k) Registro o banco de datos: conjunto organizado de datos de carácter personal, sea automatizado o no y cualquier sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.
l) Responsable del registro o banco de datos: persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de datos de carácter personal.
m) Titular de los datos: persona natural a la que se refieren los datos de carácter personal.
n) Tratamiento de datos: cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, transferir, transmitir o cancelar datos de carácter personal, o utilizarlo en cualquier otra forma.

Es importante dejar en claro que en la recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, el titular puede oponerse a la utilización de sus datos personales, pero en caso de aceptarlo, la organización deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. Además, los resultados y su comunicación deben omitir todo tipo de información que pueda ser indicio para la identificación de las personas consultadas (artículo N° 3), por lo que para el tratamiento de los datos, el titular deberá autorizar por escrito, en pleno conocimiento del propósito del almacenamiento de datos (artículo N° 4).

El artículo N° 5 expone que *"el responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes"*[49] (artículo N° 5). Este procedimiento automatizado de transmisión permitirá al responsable o a quien maneje la información limitar la información frente a un requerimiento por lo que, mediante una red electrónica, deberá dejarse constancia de:

a) La individualización del requirente;
b) El motivo y el propósito del requerimiento, y
c) El tipo de datos que se transmiten.

"La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe"[28] y ésta dependerá del tipo de información que se pida, la finalidad de la información requerida, entre otras características. No obstante, esto no aplicará para la información pública y cuando *"se transmiten*

[28] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599

datos personales a organizaciones internacionales en cumplimiento en lo dispuesto en los tratados y convenios vigentes"[29] (artículo N° 5).

"Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese cambio"[30] (artículo N° 7).

Es importante considerar que los datos personales sólo deben utilizarse para los fines para los cuales fueron recolectados, por lo que la información deberá responder con veracidad a la situación real, entregando datos exactos y actualizados (artículo N° 9). Además no podrá *"ser objeto de tratamiento de datos sensibles, salvo cuando la ley lo autorice, exista el consentimiento el titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"*[31] (artículo N° 10)

En relación a los titulares de los datos, éstos tienen el derecho a exigir al responsable del banco de datos *"la información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente"*[32]. Es también derecho de los titulares exigir la modificación, eliminación y/o bloqueo de los datos en caso de que éstos no reflejen la realidad de la situación, solicitud realizada por un procedimiento formal y gratuito que no puede ser limitado por ningún acto o convención por parte del organismo. *"En caso de que los datos eliminados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se hayan comunicados, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos"*[55] (artículos N° 11, 12 y 13). Ante una petición del titular de los datos, entonces, cualquiera sea su motivo, el responsable del registro o base de datos deberá pronunciarse dentro de dos días hábiles y en caso de denegarla, el titular de los datos tendrá de derecho a recurrir a un juez de letras solicitando amparo a los derechos expuestos anteriormente (Artículo N° 16).

Si bien lo anterior responde a los derechos de los titulares de los datos, lo dispuesto no aplicará en caso de *"solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ella impida o entorpezca el debido cumplimiento de las funciones fiscalizadores del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional"*[33] (artículo N° 15). El mismo Artículo expone además, que no aplicarán los

[29] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599
[30] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599
[31] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599
[32] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599
[33] Ministerio Secretaría General de Presidencia. Ley 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599

derechos de petición de modificación, cancelación o bloqueo en caso que la orden para almacenar la información del titular de los datos personales sea por mandato legal.

Todo lo expuesto sobre la Ley N° 19.628 sobre Protección de la Vida Privada debe ser respetado y aplicado tanto por personas naturales, organizaciones privadas y órganos de la Administración del Estado, cada vez que se recolecta, administre y almacene información personal y sensible sobre la vida privada de las personas.

Para el caso de los órganos de la Administración del Estado, la normativa expone que el tratamiento de datos sólo *"podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes"* agregando que cumpliéndose esas condiciones, el servicio no necesitará el consentimiento del titular de los datos para hacerlo (artículo N° 20).

Es importante clarificar que para el caso de los organismos públicos que *"sometan a tratamiento de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o pena"*[34].

Para cumplir con lo dispuesto en el artículo N° 20, la Ley expone que el *"Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos"*[35] el cual tendrá carácter público y en el constará el fundamento jurídico de cada uno de los bancos de datos exponiendo además, su finalidad, los tipos de datos almacenados y la descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

Además de lo anterior, el artículo N° 22 expone que el organismo público responsable del banco de datos *"proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca"*[59]

35. **Decreto Supremo N° 14, de febrero de 2014. Modifica Decreto N° 181, de 2002, que aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.**

Este decreto actualiza las funciones del Ministerio Secretaría General de la Presidencia (en adelante MINSEGPRES) relativas a materias de documentos electrónicos, firma electrónica y su certificación, adoptando estándares internacionales emitidos por organismos reconocidos en materia de seguridad de la información.

Asigna al MINSEGPRES la elaboración de propuestas técnicas que permitan estandarizar la atención al ciudadano a través de técnicas y medios electrónicos. Asimismo el citado ministerio, propondrá al Presidente de la República las normas técnicas que deberán seguir los órganos de la Administración del Estado para garantizar la publicidad, integridad, eficacia, interoperabilidad y seguridad en el uso de los documentos electrónicos.

[34] Ministerio Secretaría General de Presidencia. Ley N° 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599

[35] Ministerio Secretaría General de Presidencia. Ley N° 19.628 sobre Protección de la Vida Privada. http://www.leychile.cl/Navegar?idNorma=141599

36. **Instructivo Presidencial N° 8, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.**

Este instructivo imparte instrucciones referidas a la publicidad permanente de información relevante de los organismos de la Administración del Estado, ordenando la publicación en sus respectivos sitios web institucionales de información relativa a:

- Adquisiciones y contrataciones de bienes y servicios, que se efectúen con recursos asignados en los subtítulos 22, 29 y 31 de sus presupuestos,
- Información relativa a su personal de planta, contrata y honorarios.
- Transferencias de fondos que realicen a personas jurídicas con los recursos asignados en los subtítulos 24 y 33 de sus presupuestos.
- Leyes, reglamentos, dictámenes y circulares vigentes que conformen el marco normativo que les sea aplicable.
- Los actos y resoluciones que tengan efectos sobre terceros, mediante la publicación de los respectivos actos o resoluciones totalmente tramitadas.

37. **Circular Nº3, enero de 2007: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.**

La presente circular tiene por objeto facilitar la implementación del Instructivo Presidencial N° 8 de 2006, asignando a los jefes de servicio la responsabilidad de cumplir las medidas establecidas en el instructivo citado. Por otra parte, asigna un formato común para que todos los servicios publiquen su información en el sitio web www.gobiernotransparente.gob.cl/material. Asimismo, la información respectiva deberá estar disponible en www.[dominio_institucion].gob.cl/transparencia/dotacion.html. Además, la presente circular establece los plazos de implementación de dichas medidas anteriormente mencionadas.

38. **Ley N° 17.336, octubre de 1970: sobre propiedad intelectual. Ministerio de Educación Pública.**

La presente ley busca "*proteger los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de obras de la inteligencia en los dominios literarios, artísticos y científicos, cualquiera que sea su forma de expresión, y los derechos conexos que ella determina. El derecho de autor comprende los derechos patrimonial y moral, que protegen el aprovechamiento, la paternidad y la integridad de la obra*"[36] (artículo N° 1).

39. **Ley Nº 19.223, junio de 1993: Sobre delitos informáticos. Ministerio de Justicia.**

La presente ley tipifica las figuras penales relativas a la informática, señalando en su artículo N° 1 lo siguiente: *"El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus*

36 Ministerio de Educación. Ley N° 17.336: sobre propiedad intelectual. http://www.dipres.gob.cl/594/articles-51683_Otrasleyes_ley17336.pdf

partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.[37]"

Por otra parte, en sus artículos siguientes, señala las penas a las que se ven expuestos quienes busquen apoderarse de información, la altere, revele y difunda de forma maliciosa.

40. **Ley Nº 19.927, enero de 2004: Sobre delitos de pornografía infantil. Ministerio de Justicia.**

La presente ley modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil. En ella se detallan las penas a las que se enfrentan quienes sean condenados por estos delitos, así como las inhabilidades laborales que implica ello.

Se tipifica, además, en detalle, aquellas conductas que se consideran delito, así como las penas a las que se expone en caso de cometerlo.

Además se instruye a *"Toda institución pública o privada que por la naturaleza de su objeto requiera contratar a una persona determinada para algún empleo, cargo, oficio o profesión que involucre una relación directa y habitual con menores de edad, podrá solicitar que se le informe, para fines particulares, si ésta se encuentra afecta a la inhabilitación establecida en el artículo 39 bis del Código Penal.*

La misma información podrá ser entregada a cualquier persona que cuente con una autorización expresa de aquel cuyos antecedentes se solicitan, para los fines señalados en el inciso anterior.[38]"

37 Ministerio de Justicia. Ley N° 19.223: sobre delitos informáticos
http://www.dipres.gob.cl/594/articles-51683_Otrasleyes_ley19223.pdf
38 Ministerio de Justicia. Ley Nº 19.927, enero de 2004: Sobre delitos de pornografía infantil
http://www.leychile.cl/Navegar?idNorma=220055