Decreto 7

ESTABLECE NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD CONFORME LA LEY Nº 21.180

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Fecha Publicación: 17-AGO-2023 | Fecha Promulgación: 19-MAY-2023
Tipo Versión: Única De : 17-AGO-2023
Url Corta: https://bcn.cl/3hri8

ESTABLECE NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD CONFORME LA LEY Nº 21.180

Núm. 7.- Santiago, 19 de mayo de 2023.

Visto:

Lo dispuesto en los artículos 32 Nº 6 y 35 del decreto supremo Nº 100, de 2005, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile; en la ley Nº 19.880, que Establece Bases de los Procedimientos Administrativos que rigen los Actos de los órganos de la Administración del Estado; en la ley Nº 18.993, que Crea Ministerio Secretaría General de la Presidencia de la República; en la ley Nº 21.180, sobre Transformación Digital del Estado; en el decreto con fuerza de ley Nº 1, de 2020, del Ministerio Secretaría General de la Presidencia, que establece normas de aplicación del artículo 1º de la ley Nº 21.180, de Transformación Digital del Estado, respecto de los procedimientos administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley, a los órganos de la Administración del Estado que indica y las materias que les resulten aplicables; en el decreto supremo Nº 4, de 2020, del Ministerio Secretaría General de la Presidencia, que aprueba el reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley Nº 21.180 sobre Transformación Digital del Estado; en el decreto supremo Nº 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en el Instructivo Presidencial Nº 8, de 2018, donde se imparten instrucciones en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado; y, en la resolución Nº 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón, de las materias de personal que se indican.

Considerando:

1) Que, el artículo 1º de la ley Nº 21.180 sobre Transformación Digital del Estado modificó la ley Nº 19.880 para incorporar la digitalización y transformación del ciclo de los procedimientos administrativos.

2) Que, la misma ley encomendó a un reglamento la regulación de una serie de temas específicos, el que se materializó mediante el decreto supremo Nº 4, de 2020, del Ministerio Secretaría General de la Presidencia, que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley Nº 21.180 sobre Transformación Digital del Estado; en adelante también "el Reglamento".

3) Que, asimismo, la ley Nº 21.180 facultó al Presidente de la República para establecer, mediante uno o más decretos con fuerza de ley, la gradualidad en la implementación de la ley para los distintos órganos de la Administración del Estado. Ello se materializó a través del decreto con fuerza de ley Nº 1, de 2020, del Ministerio Secretaría General de la Presidencia.

4) Que, el Reglamento dispuso la dictación de seis normas técnicas sobre interoperabilidad, seguridad de la información y ciberseguridad, documentos y expedientes electrónicos, notificaciones, calidad y funcionamiento, y de autenticación. Estas normas deberán ser dictadas mediante decretos supremos emitidos por el Ministerio Secretaría General de la Presidencia y suscritos también por la o el Ministro (a) del Interior y Seguridad Pública, de Hacienda, de Justicia y Derechos Humanos o de las Culturas, las Artes y el Patrimonio, según corresponda.

5) Que, en tanto, conforme el mandato del artículo 37 bis de la ley Nº 19.880 y el artículo 58 del Reglamento, mediante los ordinarios Nº 1.454 de 8 de octubre de 2019, Nº 1.742 de 24 de noviembre de 2019, y Nº 128 de 28 de enero de 2021, todos del Ministerio Secretaría General de la Presidencia y el ordinario Nº 1.453 de 8 de octubre de 2020, de la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia, se citó a 26 órganos de la Administración del Estado y a la Corporación Administrativa del Poder Judicial para participar en seis mesas de trabajo interinstitucionales, cuya finalidad fue generar documentos con recomendaciones técnicas sobre el contenido de cada norma técnica.

6) Que, particularmente, la Mesa Técnica de Seguridad de la Información y Ciberseguridad contó con la participación del Ministerio del Interior y Seguridad Pública a través de su Equipo de Respuesta ante Incidentes de Seguridad Informática, el Ministerio de Defensa Nacional, la Subsecretaría de Telecomunicaciones, la Dirección de Presupuestos, la Secretaría de Modernización del Ministerio de Hacienda, el Consejo para la Transparencia, la Corporación de Fomento de la Producción y el Servicio de Impuestos Internos, quienes trabajaron de acuerdo a estándares internacionales emitidos por organismos reconocidos en esta materia, así como en base a diversas normas técnicas de uso frecuente en nuestro país.

7) Que, entre los días 17 al 31 de diciembre de 2021, el Ministerio Secretaría General de la Presidencia realizó un proceso público y participativo de consulta ciudadana, que convocó a personas y agrupaciones de la sociedad civil, para que pudieran opinar y aportar respecto del modelo de la norma técnica de calidad y funcionamiento. Dichas opiniones, así como las recogidas en la mesa técnica citada conforme al considerando 6º precedente se valoraron y se tuvieron en consideración para la elaboración final de la presente norma técnica.

8) Que, en atención a que los órganos de la Administración del Estado están obligados a disponer y utilizar plataformas electrónicas para la gestión de sus expedientes electrónicos, en virtud de las modificaciones introducidas por la Ley de Transformación Digital del Estado, es necesario establecer un proceso para resguardar la confidencialidad, integridad y disponibilidad de la información, así como proteger la infraestructura informática de las plataformas electrónicas que sustentan sus procedimientos administrativos, reforzando el cumplimiento de los principios establecidos en el artículo 16 bis nuevo de la ley Nº 19.880.

9) Que, con fecha 4 de febrero de 2022, se dictó el decreto supremo Nº 6, del Ministerio Secretaría General de la Presidencia, que establece norma técnica de notificaciones conforme la ley Nº 21.180 (sic), refiriéndose en realidad a la norma técnica de seguridad y ciberseguridad, el que fue ingresado a Contraloría General de la República para su trámite de toma de razón, con fecha 10 de marzo de 2022.

10) Que, con fecha 8 de abril de 2022, el Ministerio Secretaría General de la Presidencia hizo retiro del decreto supremo en comento, por considerar necesario revisar los contenidos de dicho acto en detalle y subsanar ciertas incongruencias, teniendo en especial consideración el específico carácter técnico del mismo, para lo cual inició un proceso de revisión del mismo con los órganos competentes.

11) Que, en virtud de lo antes expuesto y a las facultades que la ley me otorga,

Decreto:

Establézcase la siguiente Norma Técnica de Seguridad de la Información y Ciberseguridad de las Plataformas Electrónicas que sustentan procedimientos administrativos en los órganos de la Administración del Estado:

"TÍTULO PRIMERO
Disposiciones generales

Artículo 1.- Objeto. La presente norma tiene por objeto definir los estándares y establecer las directrices técnicas sobre seguridad de la información y ciberseguridad, que deberán cumplir los órganos de la Administración del Estado para resguardar la confidencialidad, integridad, disponibilidad de la información y la infraestructura informática, de las plataformas electrónicas que sustentan sus procedimientos administrativos.

Artículo 2.- Definiciones. Para fines de esta norma técnica, se entenderá por:

1) Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.
2) Activo de Información: Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.
3) Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.
4) Confidencialidad: Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.
5) Control de Seguridad: Conjunto de estándares, buenas prácticas y normativas que permiten administrar los riesgos en las tecnologías de la información.
6) Disponibilidad: Atributo de los activos y activos de información, relativo a su accesibilidad y utilización a requerimiento de una entidad o proceso autorizado.
7) Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.
8) Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.
9) Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.
10) Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.
11) Reglamento: Decreto supremo Nº 4, de 2020, del Ministerio Secretaría General de la Presidencia, que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las

materias que indica, según lo dispuesto en la ley Nº 21.180 sobre Transformación Digital del Estado.

12) Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

13) Servidor: Equipo virtual o físico dedicado a entregar servicios de red, servicios de bases de datos, sitios web, sistemas informáticos, carpetas compartidas y, en general, brindar los recursos necesarios para responder las peticiones de usuarios.

14) Sistema Informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.

15) Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

Artículo 3.- Marco para la seguridad de la información y ciberseguridad. Los órganos de la Administración del Estado deberán estructurar su trabajo a partir del diagnóstico inicial a que alude el artículo 4 definiendo funciones y categorías según lo señalado en el Título Tercero, junto con la generación e implementación de la Política de Seguridad de la Información y Ciberseguridad a que alude el artículo 5 de la presente norma técnica.

Artículo 4.- Diagnóstico inicial. Cada órgano de la Administración del Estado deberá realizar un diagnóstico inicial del estado de ciberseguridad de sus plataformas electrónicas, en conformidad a lo que dispondrán las guías técnicas mencionadas en el artículo 12 de la presente norma.

Los órganos de la Administración del Estado deberán incluir el diagnóstico realizado en virtud de este artículo en el Catálogo de Plataformas de la Norma Técnica de Calidad y Funcionamiento, señalada en el artículo 57 del Reglamento, con el fin de mantener un registro íntegro de las plataformas electrónicas que administren.

TÍTULO SEGUNDO
De la Política de Seguridad de la Información y Ciberseguridad

Artículo 5.- Política de Seguridad de la Información y Ciberseguridad. Cada órgano de la Administración del Estado deberá elaborar una Política de Seguridad de la Información y Ciberseguridad, en adelante "Política", aprobada a través de acto administrativo por el respectivo Jefe(a) Superior de Servicio, que tendrá como objetivo establecer las directrices generales en materia de seguridad de la información y ciberseguridad dentro del órgano, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan. Asimismo, deberá contener la visión estratégica del respectivo órgano de la Administración del Estado respecto de la seguridad de la información y ciberseguridad.

La Política tendrá como objetivo, además, velar por la preservación, confidencialidad, integridad y disponibilidad de la información, considerando estándares de seguridad de la información y la privacidad como parte del diseño inicial.

La Política deberá contener, a lo menos, lo siguiente:

1) Los objetivos generales específicos de la Política.

2) La identificación y determinación del alcance de la Política, atendiendo a los activos y activos de información que deben protegerse, en relación a las plataformas electrónicas que sustentan procedimientos administrativos; y los roles involucrados en el ejercicio de cada función para cumplir con dicho objetivo.

3) La legislación y normativa vigente aplicable al órgano.

4) Especificar los roles, y definir un(a) responsable institucional de seguridad de la información y ciberseguridad y un(a) responsable de los activos de información.

El (La) responsable institucional de seguridad de la información y ciberseguridad, será el (la) encargado(a) de velar por la seguridad de la información y ciberseguridad dentro del órgano de la Administración del Estado respectivo, asegurar el desarrollo, cumplimiento y actualización de la Política y de gestionar la administración de la seguridad de la información y ciberseguridad.

El (La) responsable de los activos de información, será el (la) responsable de su identificación y clasificación, así como gestionar el riesgo y niveles de seguridad asociados.

El desempeño de estas funciones no podrá ser externalizado bajo ninguna forma.

Cada órgano de la Administración del Estado deberá determinar si estos roles se unifican o no en una sola persona.

Para aquellos órganos que hayan nombrado un(a) encargado(a) de ciberseguridad, de acuerdo con lo establecido en el Instructivo Presidencial Nº 8, de 2018, se entenderá este requisito desde ya como cumplido, salvo que opten por designar un(a) nuevo(a) encargado(a).

La o las guías técnicas a las que alude el artículo 12 de la presente norma técnica, complementarán y profundizarán los detalles técnicos y operativos sobre la Política.

TÍTULO TERCERO
Funciones y categorías

Artículo 6.- Funciones y categorías. Para la generación e implementación de la Política a que se refiere el Título Segundo precedente, cada órgano de la Administración del Estado deberá atender a las funciones y categorías que se determinan en el presente título y que se especificarán en la o las guías técnicas a que se refiere el artículo 12 de la presente norma técnica.

Artículo 7.- Función de identificación. Corresponde a las actividades y procesos desarrollados por un órgano de la Administración del Estado para la identificación y adecuada administración de los riesgos de seguridad de información y ciberseguridad asociados a cada uno de los procesos, personas y plataformas electrónicas que sustentan sus procedimientos administrativos.

Esta función comprende las categorías de contexto o entorno del órgano de la Administración del Estado; gobernanza; gestión de activos de información; gestión de riesgos; y contratación y gestión de la relación con proveedores de servicios en la nube. El análisis y operatividad de estas categorías se describirán en la o las guías técnicas a las que hace referencia el artículo 12 de la presente norma.

Artículo 8.- Función de protección. Los órganos de la Administración del Estado deberán desarrollar e implementar procesos y actividades destinadas a garantizar las medidas de seguridad que favorezcan la entrega de sus servicios en forma adecuada, oportuna y segura a sus destinatarios.

Esta función implica las categorías de gestión de servidores, redes, autenticación y control de acceso a plataformas electrónicas de los órganos de la Administración del Estado; la concienciación y formación de los funcionarios de la Administración; la seguridad de los datos; los procesos para proteger la información que obra en poder de la Administración; y el registro de eventos; todas

las cuales serán definidas y determinadas en la o las guías técnicas a la que alude el artículo 12 de la presente norma técnica.

Artículo 9.- Función de detección. Los órganos de la Administración del Estado deberán desarrollar e implementar los procesos y líneas de acción necesarios para la detección oportuna de la ocurrencia de incidentes de seguridad.

Esta función incluye las categorías de análisis de eventos con el objeto de identificar posibles anomalías, fallas o eventos precursores que pudieran derivar en un incidente de seguridad; un monitoreo continuo de la seguridad, en el cual los servidores y sus plataformas electrónicas deben contar con medidas adecuadas para la protección contra código malicioso; y establecer un proceso de detección de dichos eventos. Los detalles operativos de esta función y sus categorías se describirán en la o las guías técnicas conforme a lo dispuesto en el artículo 12 de la presente norma técnica.

Artículo 10.- Función de respuesta. Los órganos de la Administración del Estado deberán desarrollar e implementar aquellos procesos y actividades necesarias para adoptar medidas técnicas y organizativas cuando se detecte un incidente de seguridad de la información y/o ciberseguridad.

Esta función contiene las categorías de planificación de respuesta ante incidentes; comunicación de acciones de respuesta; análisis de incidentes; mitigación de incidentes; y mejoras a la planificación y procesos de respuesta. Los procesos, planes, gestiones y análisis asociados a esta función se describirán y desarrollarán en la o las guías técnicas a que se refiere el artículo 12 de esta norma técnica.

Artículo 11.- Función de recuperación. Los órganos de la Administración del Estado deberán desarrollar e implementar los procesos y acciones necesarios para mantener los planes de recuperación y restablecer cualquier capacidad, plataforma electrónica, sistema electrónico, servidor, red o servicio en general, que se haya visto afectado debido a un incidente de seguridad de la información y/o ciberseguridad.

Esta función contiene las categorías de planificación de la recuperación; mejoras a la planificación y procesos de recuperación; y comunicación del estado de recuperación; todas las cuales serán descritas en detalle en la o las guías técnicas a que se refiere el artículo 12 de la presente norma técnica.

TÍTULO CUARTO
Disposiciones finales

Artículo 12.- Guía técnica. Para efectos de facilitar la implementación de la presente norma técnica, la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia, dictará una o más guías técnicas que establezcan sus aspectos operativos y procesos.

Artículo 13.- Gradualidad. La aplicación de esta norma será acorde a la gradualidad establecida en el decreto con fuerza de ley Nº 1, de 2020, del Ministerio Secretaría General de la Presidencia. A fin de facilitar su implementación, la División de Gobierno Digital definirá los lineamientos y formato en que los órganos obligados deberán llevarla a cabo.

Artículo 14.- Revisión y actualización de la norma. La presente norma técnica deberá ser revisada y actualizada, al menos, cada dos años. El plazo antes

indicado se contará desde la entrada en vigencia de esta norma técnica.

Las actualizaciones de esta norma técnica deberán tomar en consideración los aprendizajes y las dificultades de aplicación reportados por los órganos de la Administración del Estado, así como impulsar las buenas prácticas y minimizar los efectos de las prácticas incorrectas que pudieron haberse presentado.".

Anótese, tómese razón, y publíquese.- GABRIEL BORIC FONT, Presidente de la República.- Álvaro Elizalde Soto, Ministro Secretario General de la Presidencia.- Carolina Tohá Morales, Ministra del Interior y Seguridad Pública.- Mario Marcel Cullell, Ministro de Hacienda.

Lo que transcribo a Ud., para su conocimiento.- Saluda atentamente a Ud., Macarena Lobos Palacios, Subsecretaria General de la Presidencia.