Decreto 273

ESTABLECE OBLIGACIÓN DE REPORTAR INCIDENTES DE CIBERSEGURIDAD

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA; SUBSECRETARÍA DEL INTERIOR

Publicación: 02-DIC-2022 | Promulgación: 13-SEP-2022
Versión: Única De : 02-DIC-2022
Url Corta: https://bcn.cl/3llhr

ESTABLECE OBLIGACIÓN DE REPORTAR INCIDENTES DE CIBERSEGURIDAD

Núm. 273.- Santiago, 13 de septiembre de 2022.

Visto:

Lo dispuesto en el inciso quinto del artículo 1, numeral 4 del artículo 19, y artículos 24 y 32 numeral 6, todos de la Constitución Política de la República; en el DFL Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el DFL Nº 29, de 2004, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.834, sobre Estatuto Administrativo; en la ley Nº 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, y modifica diversos cuerpos legales; en la ley Nº 21.459, que establece normas sobre delitos informáticos, deroga la ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest; en la ley Nº 19.628 sobre protección de la vida privada; el decreto Nº 5.996, de 1999, del entonces Ministerio del Interior, que crea la red interna (Intranet) del Estado, modificado por el decreto supremo Nº 1.299, de 2004, que establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas; en el decreto 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 decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad; la Política Nacional de Ciberseguridad, de abril de 2017; Instructivo Presidencial Nº 8, del 23 de octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado; decreto supremo Nº 579, de 2019, del Ministerio del interior y Seguridad Pública, que modifica el decreto supremo Nº 533, de 2015; lo dispuesto en la resolución Nº 7, de 2019, de la Contraloría General de la República; y conforme las facultades y atribuciones que me confiere la ley;

Considerando:

1. Que, la seguridad del país y la protección de la población son un deber del Estado, conforme a lo dispuesto en el artículo 1, inciso 5º, de la Constitución Política de la República, misma que, en su artículo 19 Nº 4, asegura a todas las personas el respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. Por consiguiente, es deber del Estado velar por los derechos de las personas en el

ciberespacio;

2. Que, el desarrollo y la masificación en el uso de las tecnologías de información y comunicaciones conlleva riesgos asociados, que eventualmente podrían afectar los derechos de las personas, las infraestructuras críticas de la información y los intereses del país, a nivel nacional e internacional. Estos riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave a la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad nacional;

3. Que, el programa de Gobierno 2022-2026 contempla la protección de la información y ciberseguridad, tanto de la información privada como pública, para lo cual se establece la implementación robusta de la Política Nacional de Ciberseguridad (en adelante "Política"), que es el instrumento de planificación del Estado de Chile en materia de ciberseguridad, la cual tiene por objeto contar con un ciberespacio libre, abierto, seguro y resiliente;

4. Que, la Política recomienda definir capacidades de levantamiento, estandarización e integración de datos e información relacionados con el cibercrimen, aumentar la capacidad para investigar y generar evidencia respecto al mismo;

5. Que, en este contexto, se debe tener presente que el Estatuto Administrativo, en su artículo 61, literal k) establece como una obligación de los funcionarios públicos la de denunciar, con la debida prontitud, los crímenes o simples delitos y, a la autoridad competente, los hechos de carácter irregular de que tengan conocimiento en el ejercicio de sus funciones;

6. Que, por su parte, la ley Nº 21.459, sobre delitos informáticos, tipifica como delitos los ciberataques que afecten a la integridad de los sistemas y/o datos informáticos, así como el acceso ilícito;

7. Que, en este orden de ideas, la prevención, la disuasión, el control y la sanción de los ilícitos son indispensables para minimizar los riesgos y amenazas en el ciberespacio, de manera de contribuir a la generación de confianza en las actividades que en él se desarrollan;

8. Que, la necesidad de contar con información que permita la prevención y gestión de riesgos del ciberespacio, y de fortalecer la capacidad de Chile para responder ante incidentes de ciberseguridad que se presenten, hace urgente la implementación de estándares de ciberseguridad más fuertes en los organismos de la administración del Estado, con el objeto de proteger las redes, plataformas y sistemas informáticos del gobierno.

9. Que, adicionalmente, con la entrada en vigencia de la ley Nº 21.459, ya referida, se hace necesario fortalecer las disposiciones vigentes en la materia, estableciendo medidas transversales a la Administración, que tengan por objeto dar protección integral los sistemas informáticos del Estado y la información contenida en ellos;

10. Que, lo anterior resulta especialmente relevante, considerando la rapidez y mutabilidad de las amenazas en el ciberespacio, que obligan a revisar permanentemente las medidas establecidas para mejorar los estándares de ciberseguridad de nuestro país, y generar instancias de coordinación intersectorial que permitan a los órganos de la administración del Estado dar una respuesta oportuna a las nuevas amenazas que se generen.

11. Que, conforme a lo establecido en los artículos 3 y 5 de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos, debiendo además los órganos del Estado cumplir sus cometidos de manera coordinada propendiendo a la unidad de acción.

Decreto:

Artículo 1º. Notificación de incidentes de ciberseguridad. Los jefes de servicio de los Ministerios y demás organismos de la Administración centralizada y descentralizada del Estado deberán comunicar los incidentes de ciberseguridad que

les afecten, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática ("CSIRT"), en el sitio web: https://csirt.gob.cl.

Artículo 2º. Plazo para la notificación. La comunicación anterior deberá realizarse tan pronto se constate su ocurrencia, no pudiendo ser este plazo superior a 3 horas desde que se tome conocimiento.

Artículo 3º. Información sobre amenazas a los órganos de la administración del Estado. Los jefes de servicio establecidos en el artículo 1, dentro del ámbito de sus facultades, y respecto de los contratos que se celebren con posterioridad a la entrada en vigencia del presente decreto, deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.

Artículo 4º. Búsqueda preventiva de vulnerabilidades. Para mejorar la seguridad de las redes y sistemas informáticos de su respectiva institución, los jefes de servicio indicados en el artículo 1º, pueden solicitar a los equipos técnicos del CSIRT su revisión y análisis, incluyendo la búsqueda preventiva de vulnerabilidades informáticas, otorgando las facilidades que sean necesarias para ello.

Anótese, tómese razón y publíquese.- GABRIEL BORIC FONT, Presidente de la República.- Carolina Tohá Morales, Ministra del Interior y Seguridad Pública.- Ana Lya Uriarte Rodríguez, Ministra Secretaria General de la Presidencia.

Lo que transcribo a Ud. para su conocimiento.- Atentamente, Manuel Zacarías Monsalve Benavides, Subsecretario del Interior.