Agencia
Nacional de
Investigación
y Desarrollo
Ministerio de Ciencia,
Tecnología, Conocimiento
e Innovación

Guía Técnica

Implementación de tecnologías para la identificación y discriminación de evidencias en la Escena del Crimen relacionada con armas de fuego.

Moneda nº1375,
Santiago, Chile
Tel: 56 (2) 2365 4600
www.anid.cl
@AnidInforma

Gobierno de Chile

Tabla de contenido

1. Contexto de los Desafíos Públicos

Desafíos Públicos es un programa que apoya a organismos del Estado a encontrar soluciones a Desafíos de interés público que requieran Investigación, Desarrollo (I+D) y/o desarrollo tecnológico para ser resueltos y generar un impacto positivo en el desarrollo económico, ambiental y social a nivel país. El programa es una manera de enfrentar problemas complejos que requieren aproximaciones transdisciplinarias y multisectoriales para ser abordados íntegramente. Desde un rol coordinador el Estado fomenta activamente el desarrollo tecnológico e innovación orientados a dar solución a los Desafíos públicos que el país presenta y que afectan a su población ya sea a nivel local, regional o nacional.

Por medio de una metodología de Desafíos, el programa busca desarrollar soluciones a problemas de interés público en ámbitos de acción de organismos públicos mediante Concursos de Innovación Abierta para emprendedoras/es, Startups, equipos universitarios, empresas, entre otros. Cada concurso financia una carrera de desarrollo de prototipos para lograr una aplicación industrial lista para implementar y que el Organismo Público pueda adquirir.

El programa es gestionado en conjunto por el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (MinCiencia), el Laboratorio de Gobierno del Ministerio de Hacienda (LabGob) y la Agencia Nacional de Investigación y Desarrollo (ANID).

El presente instrumento busca contribuir a encontrar soluciones innovadoras a problemas de interés público que requieran de un desarrollo tecnológico e innovación, conectando a quienes demandan estas soluciones, en este caso la Policía de Investigaciones de Chile (PDI) con potenciales oferentes provenientes del sistema nacional de innovación.

En particular, el problema de interés público que se requiere resolver se denomina Implementación de tecnologías para la identificación y discriminación de evidencias en la Escena del Crimen relacionada con armas de fuego, cuyo objetivo es implementar soluciones tecnológicas portátiles y mínimamente invasivas, que permitan detectar e identificar restos sanguíneos y/o residuos de disparos inorgánicos "in situ", en Escenas del Crimen vinculadas con delitos cometidos con armas de fuego.

La función de esta Guía Técnica es orientar a las personas usuarias en la elaboración de su postulación a la convocatoria de Desafíos Públicos 2024: Implementación de tecnologías para la identificación y discriminación de evidencias en la Escena del Crimen relacionada con armas de fuego, entregando información relevante para ser utilizada en la formulación.

En conjunto con esta Guía Técnica, se acompañarán las Bases del instrumento "**Desafíos Públicos 2024"** y que contienen todas las directrices y normativas respecto del proceso de postulación, admisibilidad, evaluación, seguimiento, cierre de los proyectos y temas administrativos que no forman parte de la Guía Técnica.

2. Antecedentes de la Convocatoria para el lanzamiento de los Concursos de Desafíos Públicos

Según la encuesta CEP 90, publicada el 24 de abril de 2024, la seguridad pública es una de las principales preocupaciones de los chilenos. Más aún, de acuerdo con el informe del mes de febrero de 2024 "Preocupaciones del mundo", elaborado por la empresa IPSOS, entre los países encuestados, Chile se posicionó como el país más preocupado por el crimen y la violencia con un 69%. Esta percepción encuentra un correlato con los de la última Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC 2022), confirmando que Chile llegó a sus índices más altos en cuanto a la percepción de inseguridad en una década, con un 90,6%. Más aún, la misma versión de dicha encuesta revela un incremento en la victimización a personas en el país por delitos de mayor connotación social, empinándose desde el año 2022 en adelante, hacia valores prepandémicos.

Por otra parte, el 1° Informe nacional de homicidios consumados (período 2018-2022), confirmó un fuerte aumento de los homicidios en esos cinco años, esto es, de 845 casos anuales a 1.322. Al desagregar esta cifra, se observa un importante incremento de los homicidios sin autor conocido, de un 23% en el año 2018 a un 41% en el año 2022, lo que podría interpretarse como una señal del crecimiento en la actividad del crimen organizado en el país.

Si bien, Chile registra tasas de homicidios más bajas que otros países de la región, ha venido experimentando un alza en la comisión de este tipo de delitos, registrando sólo una leve disminución durante el primer semestre de 2023. De acuerdo con el último Informe Nacional de Víctimas de Homicidios Consumados en Chile, durante el primer semestre de 2023 se registró una tasa de 3,2 víctimas de homicidios consumados cada 100 mil habitantes, lo que representa una disminución de -3,0% respecto del primer semestre de 2022. Sin embargo, estas cifras distan mucho de las magnitudes anteriores a la pandemia por COVID-19; en efecto, durante el año 2019 la tasa de homicidios fue de 2,2 personas cada 100 mil habitantes.

Respecto a lo anterior, se señala que el 52,9% de las víctimas de homicidios consumados fue agredida con arma de fuego, y según datos disponibles en la página web del Ministerio Público, durante el año 2023 un 36,9% de homicidios, se asociaron a delitos de crimen organizado.

Por otra parte, en Chile, la transición desde un sistema de administración de justicia inquisitivo a uno acusatorio ha puesto en el centro del sistema de persecución penal a la prueba científica. En ese sentido, los pilares históricos de la investigación criminal han sido modificados en una multitud de aspectos, lo que implica que las pruebas valen por el grado de convicción que genera en el juzgador dentro de los límites establecidos. En ese contexto, la Policía de Investigaciones de Chile (PDI), por definición la policía científica del país juega un rol fundamental en el esclarecimiento de los delitos y en la

consecución de condenas efectivas que contribuyan a combatir la sensación de impunidad en la ciudadanía.

La PDI está al servicio de la comunidad y sus acciones se orientarán a la investigación especializada de todos los delitos, especialmente aquellos complejos y relacionados con el crimen organizado, contribuyendo a evitar la perpetración de hechos delictuosos y de actos atentatorios contra la estabilidad de los organismos del Estado. Con el objetivo de adecuarse permanentemente a los cambios delictuales, la Policía de Investigaciones de Chile, ha venido incorporando desde hace ya varios años, diversos lineamientos estratégicos a su gestión, integrando objetivos específicos destinados a fortalecer el trabajo del área forense y con ello, la prueba científica. Sin ir más lejos, el actual Plan Estratégico de Desarrollo Policial, PEDP 2023 – 2028, contempla entre los procesos internos claves que deben ser desarrollados por la PDI, potenciar la investigación profesional y especializada sustentada en evidencia criminalística.

En el actual contexto criminal, especialmente en lo relacionado con delitos de homicidios y otros delitos violentos asociados al uso de armas de fuego, la falta de técnicas lo suficientemente robustas para la identificación "in situ" de restos sanguíneos y residuos de disparos de origen inorgánico en orificios de prendas de vestir u otras matrices tales como murallas, metales, entre otros, incide en el levantamiento de grandes volúmenes de indicios, aun cuando no todos estos resultan de utilidad para la investigación. Esta situación, sumado a los prolongados tiempos requeridos para la ejecución de los análisis forenses tradicionales de laboratorio, pueden incidir en la oportunidad de los informes periciales, al prolongar los tiempos de respuesta, pudiendo incluso afectar la eficiencia y la efectividad de la persecución penal.

Por otra parte, la imposibilidad de contar con resultados confiables durante el procesamiento de la Escena del Crimen dificulta la rápida toma de decisiones por parte de detectives y fiscales. Estos nudos entorpecen la implementación de mecanismos de inteligencia e integración forense, lo que se traduce en que parte de los esfuerzos y recursos que el Estado invierte en la resolución de delitos violentos, se diluyen, debido a que muchas veces resulta imposible orientar con mayor intensidad las indagaciones, hacia líneas investigativas concretas.

Si bien es cierto, la problemática planteada corresponde a un desafío impuesto a la gran mayoría de los laboratorios forenses, prácticamente todos estos siguen utilizando métodos orientativos para el levantamiento de las evidencias en la Escena del Crimen. No obstante, durante el último tiempo, se han comenzado a explorar algunas técnicas analíticas, con la finalidad de detectar e identificar indicios relacionados con artefactos explosivos y drogas en el Sitio del Suceso. Entre las tecnologías desarrolladas y comercialmente disponibles, se encuentran equipamientos basados en técnicas vibracionales, en específico, equipos portátiles Raman e Infrarrojo, los cuales, de acuerdo con sus características de configuración, tipo de evidencia y cantidad de esta, exhiben variaciones en su respuesta analítica, afectando incluso su robustez. De igual

manera, ha habido intentos de traspasar la tecnología utilizada para la detección de agentes químicos de compuestos orgánicos volátiles y semivolátiles (VOC/SVOC) en la fase vapor, en especial para la detección de compuestos relacionados con artefactos explosivos mediante tecnologías de separación química acoplada a Espectroscopía Infrarroja Fotoacústica (GC-QEPAS). Estos intentos aún no han podido cristalizar en soluciones comercialmente disponibles.

Otro tipo de metodología que ha sido explorada en la investigación forense es la utilización de Imágenes Hiperspectrales (HSI), en concreto, para la discriminación de evidencias químicas como drogas y explosivos y, en el caso de evidencias biológicas, se ha empleado en el análisis de sangre, semen, fluido vaginal y orina. Sin embargo, los equipamientos desarrollados para estas aplicaciones aún presentan inconvenientes que impiden su uso masivo.

Desde el año 2020, un grupo de investigadores de la Comunidad Europea ha levantado un proyecto de carácter internacional denominado "RISEN" (Real-time on-site forensic trace qualification), cuyo objetivo es desarrollar sensores sin contacto, destinados a identificar en tiempo real, distinto tipo de evidencias en la Escena del Crimen. El proyecto RISEN se encuentra en la fase final de ejecución y los sensores desarrollados, no están comercialmente disponibles. dichos dispositivos se basan en métodos espectroquímicos y físicos que incluyen, espectroscopía Raman, infrarroja, espectrometría de movilidad iónica (IMS), cámaras multi hiperspectrales de amplio rango (HSI), sensores de dispersión láser/fluorescencia inducida por láser (LS/LIF), espectroscopía de fractura inducida por láser (LIBS) entre otros. Sin embargo, es muy importante precisar que la filosofía tras este proyecto consiste en trasladar la detección de señales a la Escena del Crimen no así la identificación propiamente tal. Dado aquello, mientras personal técnico opera los sensores en terreno, expertos deben permanecer en dependencias del laboratorio, para analizar los datos que les son transmitidos por los equipos de campo.

3. Objetivo y resultados esperados

El objetivo general de la convocatoria enmarcado en el instrumento Desafíos Públicos es:

Implementar soluciones tecnológicas portátiles y mínimamente invasivas, que permitan detectar e identificar restos sanguíneos y/o residuos de disparos inorgánicos "in situ", en Escenas del Crimen vinculadas con delitos cometidos con armas de fuego. Lo anterior, a través de un proceso de innovación abierta que convoque las mejores capacidades del sistema de ciencia e innovación.

Los resultados globales esperados para esta etapa son:

1. Tecnología portátil mínimamente invasiva, adaptada para su utilización en la Escena del Crimen, que sea capaz de identificar y discriminar con especificidad, sensibilidad y confiabilidad sangre (visible y/o latente) y/o residuos de disparos inorgánicos en vestimentas y/u otras matrices tales como concreto, estructuras metálicas, superficies de vehículos, validada en terreno.

Se espera que las soluciones tecnológicas tengan los siguientes atributos, que permita abordar el Desafío:

1. **Exactitud**: La información que se genere a partir de la materialidad de las evidencias debe ser lo suficientemente exacta para la toma de decisiones en la Escena del Crimen. El nivel de exactitud aceptado será aquel que alcance o sea mayor que el 80%, empleando protocolos de validación típicos para técnicas analíticas.

2. **Mínimamente invasivo:** Las herramientas tecnológicas deben garantizar la mínima intervención de los indicios durante todas las etapas del análisis en terreno, al objeto de preservar la naturaleza e integridad de las evidencias durante el proceso de análisis.

3. **Portable**: Las tecnologías desarrolladas deben ser lo suficientemente compactas (de reducido tamaño y peso razonable, que permita una fácil maniobrabilidad) como para poder ser transportadas junto con el equipo de especialistas hasta la Escena del Crimen. Así mismo, deben poseer una autonomía de larga duración, de a lo menos cuatro horas de uso, para ser empleados en lugares sin acceso a electricidad.

Deseablemente se espera que además de lo anterior, las tecnologías cuenten con métodos y patrones de verificación/calibración "in situ", que garanticen su óptimo funcionamiento en terreno.

4. Consideraciones para el acceso a la solución final o transferencia y masificación de los resultados

Si las soluciones tecnológicas desarrolladas por el oferente que adjudique el presente desafío satisfacen los requerimientos establecidos la PDI en esta Guía Técnica, deberá concretarse la transferencia de estas a la Policía de Investigaciones de Chile, con la finalidad que la institución pueda hacer uso de estas, bajo las siguientes consideraciones:

- Si las tecnologías que resuelven el desafío público alcanzan el nivel de Demostración en un entorno operativo real (TRL7), Sistema completo y calificado en ambiente operacional (TRL8) y/o superior, el monto total de adquisición de dichas tecnologías por parte de la PDI, deberá ser preferente y siempre inferior al valor con que la empresa que desarrolle la solución o la organización a quién ceda los respectivos derechos, patentes, licencias u otras, comercialice estos equipamientos a terceros. A cambio de lo anterior, el equipo innovador podrá continuar escalando su solución tecnológica, valiéndose de los aportes realizados por la PDI especificados en la presente Guía Técnica.

- Si una vez finalizado el programa correspondiente a la presente convocatoria, el equipo emprendedor que desarrolle la solución o en su defecto, la organización a quién éste ceda los respectivos derechos, patentes, licencias u otras, desea continuar escalando la tecnología, lo hará a su propio costo o mediante fondos concursables disponibles en ese momento. En cualquier caso, el escalamiento considerará el trabajo conjunto con la PDI, apegándose a los puntos establecidos en el presente documento.

5. Detalle de Etapas

La presente convocatoria tendrá 03 Etapas que se llevarán a cabo en forma consecutiva, las cuales se denominan:

- Etapa 1: Validación de Entornos relevantes
- Etapa 2: Validación de Entornos simulados
- Etapa 3: Implementación y/o escalabilidad demostrada en entorno real

En cada una de las Etapas se desarrollarán actividades conducentes a alcanzar los resultados esperados en ellas. Asimismo, cada Etapa tendrá un número de proyectos seleccionados, los que serán indicados en este mismo apartado.

A continuación, se detallan las Etapas que contendrá la presente convocatoria:

Etapa 1: Validación de Entornos Relevantes

1.1 Inicio de la Etapa 1:

El proceso de admisibilidad, evaluación y adjudicación de los proyectos que ingresen a la Etapa 1, se regirá de acuerdo con lo indicado en el numeral "Evaluación de los Proyectos" de las bases de Desafíos Públicos 2024.

Al momento de la postulación, cada postulante deberá contar con un prototipo validado a nivel de laboratorio. Para la presente convocatoria se entenderá como prototipo validado en laboratorio a las herramientas tecnológicas de mesón o portátil desarrolladas que sean mínimamente invasivas y que permitan identificar residuos biológicos y/o residuos inorgánicos tales como plomo, cobre, bario, antimonio, zinc, entre otros.

1.2 Resultado de la Etapa 1:

Se espera que el prototipo cumpla, con al menos, los siguientes requisitos/parámetros/atributos:

1. **Mínimamente invasivo**: Las herramientas tecnológicas deberán ser no destructivas o mínimamente invasivas a objeto de preservar la naturaleza de las evidencias en todo el proceso investigativo.

2. **Exactitud de los resultados igual o superior al 80%**: Las herramientas tecnológicas deberán ser capaces en esta etapa, de identificar con exactitud, sustancias como sangre y/o residuos inorgánicos derivados de proyectiles balísticos o del primer de una munición, compuestos por plomo, bario, antimonio, estaño y/u otros elementos asociados a cartuchos balísticos.

Es preciso indicar en este punto que, en las etapas posteriores, se espera que el prototipo desarrollado además sea portable (fácilmente transportable).

Por tanto, el resultado esperado para esta Etapa será, un prototipo validado en entornos relevantes o simulados, lo que se entenderá como:

Herramientas tecnológicas mínimamente invasivas capaces de identificar con exactitud igual o superior al 80% de sustancias biológicas como la sangre y/o residuos inorgánicos de un proceso de disparo, sin destruir ni alterar los materiales examinados durante el proceso de análisis.

1.3 Plazos de la Etapa 1:

Las actividades de esta Etapa deberán desarrollarse dentro de un plazo máximo de 6 meses.

Para avanzar a la siguiente Etapa todos los proyectos adjudicados en la Etapa 1 deben presentar un informe de resultados y propuesta de continuidad a la Etapa 2 antes del término de la Etapa 1. Junto con esto, deberán declarar todos los gastos correspondientes al presupuesto ejecutado en la Etapa 1.

1.4 Número de proyectos a adjudicar en la Etapa 1:

La presente convocatoria adjudicará en esta Etapa hasta 6 proyectos.

1.5 Monto de subsidio para cada proyecto en la Etapa 1:

El monto de subsidio para cada proyecto adjudicado para la Etapa 1 es de hasta $40.000.000. El costo total de la Etapa del proyecto debe cumplir con los requisitos de financiamiento y aportes de acuerdo con lo establecido en el numeral "Financiamiento, aportes del Beneficiario y Asociada(s)" de las bases de los Desafíos Públicos 2024.

1.6 Aportes de la Policía de Investigaciones de Chile en la Etapa 1:

Para la Etapa 1 los proyectos adjudicados podrán tener acceso a:

- Apoyo de la Jefatura Nacional de Criminalística a través de reuniones presenciales o remotas para aclarar aspectos jurídicos y administrativos del funcionamiento de la labor forense que realiza la PDI.
- Apoyo del Laboratorio de Criminalística Central a través de reuniones presenciales o remotas para aclarar aspectos operativos del trabajo en la Escena

del Crimen, el resguardo de la evidencia y características de las evidencias biológicas y balísticas derivadas de delitos cometidos con armas de fuego

- Se podrán proporcionar distintas matrices que contengan residuos de disparos inorgánicos como es el caso de vestimentas u otras.
- Retroalimentación a los aportes de avance.
- Acercamiento con las instalaciones del Laboratorio de Criminalística Central para coordinar actividades, que permitan mejorar la especificidad y selectividad de la información que se incorporen para los prototipos.

Etapa 2: Validación de Entornos Simulados

2.1 Inicio de la Etapa 2:

El proceso de evaluación y selección de proyectos que ingresen en la Etapa 2, será lo indicado en el numeral "Informe de continuidad y evaluación de continuidad entre etapas" de las bases de los Desafíos Públicos 2024.

Cada postulante deberá contar, al momento del inicio de la Etapa 2, con un prototipo validado a nivel entornos relevantes/simulados, que corresponde al resultado obtenido en la etapa 1.

2.2 Resultado de la Etapa 2:

Se espera que el prototipo cumpla con, al menos, los siguientes requisitos/parámetros/atributos:

1. **Sensibilidad de los resultados**: las tecnologías deben ser capaces de identificar "in situ" con una sensibilidad razonable para cada tipo de sustancia, materiales biológicos como restos de sangre y residuos inorgánicos derivados de la descarga de armas de fuego (elementos del primer y/o de la munición).

    1.1 Para muestras de manchas de sangre, la sensibilidad debe alcanzar un nivel de detección 1/32000 o mejor (en referencia a lo determinado con Bluestar® Forensics).

    1.2 Para muestras de residuos inorgánicos, la sensibilidad debe alcanzar niveles de 500 ppb o mejor.

2. **Diseño del equipo:** Los prototipos deben ser portables con un tamaño y peso reducido que facilite el transporte por el usuario, sin causar molestias ergonómicas. Además, deben poseer una autonomía de larga duración, de a lo menos seis horas de uso, para ser empleados en lugares sin acceso a electricidad. Por último, su funcionamiento no deberá verse afectado por cambios en las condiciones ambientales:

    2.1 Debe funcionar correctamente en un amplio rango de temperaturas, de a lo menos entre -5 C° y 40 °C, sin perder precisión ni sensibilidad.

2.2 Debe ser estable frente a cambios rápidos de temperatura ambiente (1 °C cada 30 minutos).

2.3 Debe poseer una carcasa que le otorgue resistencia contra golpes o caídas.

2.4 Que sean resistentes al polvo y a la humedad

Deseablemente, además la tecnología desarrollada debe compensar la altitud.

Por tanto, el resultado esperado para esta Etapa será un prototipo validado en entornos reales, que se entenderá como:

Equipos portátiles mínimamente invasivos, de tamaño y peso apropiados para el transporte y operación en terreno, con autonomía de a lo menos seis horas, que sean resistentes al polvo y a la humedad, capaces de realizar análisis en un amplio rango de temperatura, sin perder precisión ni sensibilidad y de ser estables frente a cambios rápidos de temperatura ambiente, resistentes a los golpes, con protocolos de verificación/calibración en terreno. La validación de las características de los equipos portátiles en esta etapa se realizará en una Escena del Crimen simulada.

2.3 Plazos de la Etapa 2:

Las actividades de esta Etapa deberán desarrollarse dentro de un plazo máximo de 6 meses.

Para avanzar a la siguiente Etapa, todos los proyectos adjudicados en la Etapa 2 deben haber presentado su informe de resultados y su propuesta de continuidad para la Etapa 3 antes del término de la Etapa 2. Junto con esto, deberán haber declarado todos los gastos correspondientes al presupuesto ejecutado en la Etapa 2.

2.4 Número de proyectos a adjudicar en la Etapa 2:

La presente convocatoria adjudicará en esta Etapa 4 proyectos.

2.5 Monto de subsidio para cada proyecto en la Etapa 2:

El monto de subsidio por cada proyecto adjudicado para la Etapa 2 es de hasta $80.000.000 El costo total de la Etapa del proyecto debe cumplir con los requisitos de financiamiento y aportes de acuerdo con lo establecido en el numeral “Financiamiento, aportes del Beneficiario y Asociada(s)” de las bases de los Desafíos Públicos 2024.

2.6 Aportes de Policía de Investigaciones de Chile en la Etapa 2:

Para la Etapa 2 los proyectos adjudicados podrán tener acceso a:

- Apoyo de la Jefatura Nacional de Criminalística a través de reuniones presenciales o remotas para aclarar aspectos jurídicos y administrativos del funcionamiento de la labor forense que realiza la PDI.
- Apoyo del Laboratorio de Criminalística Central a través de reuniones presenciales o remotas para aclarar aspectos operativos del trabajo en la Escena del Crimen, el resguardo de la evidencia y características de las evidencias biológicas y balísticas derivadas de crímenes violentos para ser analizadas.
- Acercamiento a instalaciones de la PDI, como polígonos de tiro, con el propósito de generar matrices reales, tales como prendas de vestir con orificios balísticos, residuos de disparo en superficies de concreto y residuos de disparo en superficies metálicas.
- Participación en una Escena del Crimen simulada, relacionada con la comisión de un delito que involucra el uso de armas de fuego.
- Verificar por parte del Laboratorio de Criminalística Central, los resultados obtenidos por las propuestas de soluciones tecnológicas, a partir de matrices reales, tales como sangre visible y/o latente adherida a distintos soportes de interés forense.
- Retroalimentación a los aportes de avance.
- Acercamiento con las instalaciones del Laboratorio de Criminalística Central para coordinar actividades, que permitan mejorar la especificidad y selectividad de la información que se incorporen para los prototipos.

Etapa 3: Implementación y/o escalabilidad demostrada en entorno real

3.1 Inicio de la Etapa 3:

El proceso de evaluación y selección de proyectos que ingresen en la Etapa 3, será lo indicado en el numeral "Informe de continuidad y evaluación de continuidad entre etapas" de las bases de los Desafíos Públicos 2024.

Cada postulante deberá contar al momento del inicio de la Etapa 3 con un prototipo validado en entorno simulado. Para la presente convocatoria se entenderá como prototipo validado en entorno simulado a los resultados obtenidos en la etapa 2.

Los prototipos que se desarrollen durante la Etapa 3 deberán ser validados mediante su uso en entornos reales. Para ello los postulantes deberán capacitar al personal científico-técnico del Laboratorio de Criminalística de la PDI, para el uso en terreno de los prototipos desarrollados, quienes realizarán tres pruebas durante esta etapa, con la finalidad de contrastar sus resultados con los métodos instrumentales instalados en los laboratorios.

3.2 Resultado de la Etapa 3:

Se espera que la implementación y/o escalabilidad cumpla con al menos los siguientes requisitos/parámetros/atributos:

1 **Robustez de los resultados**: Las tecnologías desarrolladas e implementadas en esta etapa, deberán deben ser lo suficientemente robustas ante las variaciones de las condiciones del medio, lo anterior determinado a través de la metodología de Youden y Steiner para evaluar el impacto de las variables ambientales sobre los resultados obtenidos. Es deseable que la diferencia entre los valores máximos y los valores mínimos de la variable en estudio sea superior a $\sqrt{2}$ de la desviación estándar de los replicados. Lo anterior, adicionalmente a los parámetros de exactitud y sensibilidad alcanzados en las etapas anteriores.

2 **Rapidez en la adquisición y procesamiento de datos:** Las tecnologías implementadas deben en un tiempo breve, adquirir y procesar la información recolectada, a fin de obtener la identificación o el interpretación de los resultados en un tiempo menor a 5 minutos por muestra.

3 **Valores predictivos apropiados contrastados con métodos analíticos instalados en el Laboratorio**: Las tecnologías portátiles desarrolladas deberán cumplir con valores predictivos negativos del 90% o superiores, contrastados con las técnicas utilizadas en el Laboratorio. De igual forma, deberán alcanzar valores predictivos positivos del 50% o superiores, al compararse con los métodos establecidos.

Deseablemente, para evaluar la calidad de los resultados obtenidos por los desarrolladores, se espera contar con los siguientes atributos:

1.1 Selectividad: Las tecnologías implementadas deben ser selectivas en el sentido de que sus resultados no sean afectados por la presencia de componentes interferentes que se encuentren normal o frecuentemente de las matrices estudiadas.

1.2 Linealidad: Las tecnologías implementadas deben entregar resultados que sean proporcionales a la cantidad de analitos presentes en la matriz, deseablemente alcanzando un grado de respuesta medido por coeficiente de correlación >0,99.

1.3 Precisión: Las tecnologías implementadas deben entregar resultados precisos expresados en términos de repetibilidad y reproducibilidad, con valores de coeficiente de variación de Horwitz (para trazas) no superior al 20%.

1.4 Veracidad: Las tecnologías desarrolladas implementadas deben entregar resultados veraces, expresados en términos del sesgo respecto de un material de referencia, con valores que se encuentren en un rango ± 20% del valor esperado.

Por tanto, el resultado de esta Etapa será la implementación y/o escalabilidad demostrada en entorno real, que se entenderá como:

Equipos portátiles mínimamente invasivos, de tamaño y peso apropiados al transporte en terreno, con autonomía de hasta lo menos cuatro horas, que sean resistentes al polvo y a la humedad (IP 67 o mejor), capaces de realizar análisis en un amplio rango de temperatura, sin perder precisión ni sensibilidad y de ser estables frente a cambios rápidos de temperatura ambiente, resistentes a los golpes, con protocolos de verificación/calibración en terreno.

3.3 Plazos de la Etapa 3:

Las actividades de esta Etapa deberán desarrollarse dentro de un plazo máximo de 12 meses.

3.4 Número de proyectos a adjudicar en la Etapa 3

La presente convocatoria adjudicará en esta Etapa 2 proyectos.

3.5 Monto de subsidio para cada proyecto en la Etapa 3:

El monto de subsidio para cada proyecto adjudicado para la Etapa 3 es de hasta $120.000.000. El costo total de la Etapa del proyecto debe cumplir con los requisitos de financiamiento y aportes de acuerdo numeral "Financiamiento, aportes del Beneficiario y Asociada(s)" de las bases de los Desafíos Públicos 2024.

3.6 Aportes de Policía de Investigaciones de Chile en la Etapa 3:

Para la Etapa 3 los proyectos adjudicados podrán tener acceso a:

- Apoyo de la Jefatura Nacional de Criminalística a través de reuniones presenciales o remotas para aclarar aspectos jurídicos y administrativos del funcionamiento de la labor forense que realiza la PDI.
- Apoyo del Laboratorio de Criminalística Central a través de reuniones presenciales o remotas para aclarar aspectos operativos del trabajo en la Escena del Crimen, el resguardo de la evidencia y características de las evidencias biológicas y balísticas derivadas de crímenes violentos para ser analizadas.
- Verificar en Escenas del Crimen por parte del Laboratorio de Criminalística Central, los resultados obtenidos por las propuestas de soluciones tecnológicas, a partir de matrices reales, tales como sangre visible y/o latente adherida a distintos soportes de interés forense, prendas de vestir con orificios balísticos, residuos de disparo en superficies de concreto y residuos de disparo en superficies metálicas.
- Retroalimentación a los aportes de avance.

- Acercamiento con las instalaciones del Laboratorio de Criminalística Central para coordinar actividades, que permitan mejorar la especificidad y selectividad de la información que se incorporen para los prototipos.
- Pruebas en terreno por parte del personal experto PDI, usando la tecnología diseñada por el equipo innovador y comparación de resultados con las actuales pruebas que se usan en terreno para identificación de restos de sangre y/o residuos inorgánicos de un proceso de disparo.

6. Consideraciones de la Policía de Investigaciones de Chile para el desarrollo del proyecto

1 En relación a la obligación de **confidencialidad**, el postulante se obliga a la más absoluta y total reserva de información, procedimiento, fórmula técnica, documentación, archivos informáticos y en general, cualquier antecedente obtenido de la Policía de Investigaciones de Chile, con ocasión de este concurso, quedando expresamente prohibido divulgarlos, publicarlos, fotocopiarlos, copiarlos o distribuirlos a terceros extraños. La obligación se hace extensiva al personal de su dependencia, consultores, subcontratistas y dependientes de subcontratistas y se mantendrá aún después de verificado el cumplimiento cabal y pleno de sus obligaciones. Respecto de los datos que el contratista tenga acceso en virtud de la ejecución del proyecto, deberá aplicar los estándares de seguridad establecidos en el Decreto N° 83, de 2004 del Ministerio Secretaría General de la Presidencia -sobre seguridad y confidencialidad de los documentos electrónicos-, y no los podrá recolectar, almacenar, transferir, transmitir, comunicar, tratar, ceder o usar de cualquier forma, salvo que dichas acciones sean necesarias para el cumplimiento de las obligaciones consignadas en el acuerdo y/o que medie una autorización escrita por parte del representante legal de la PDI. A su vez, y en relación con información que sea absolutamente confidencial, el postulante no podrá mantenerlos en su poder, debiendo eliminar en forma irreversible cualquier copia de dicha información que disponga en sus registros lógicos y físicos. Todo lo anterior sin perjuicio de las normas de transparencia y publicidad que informan los procesos de licitaciones públicas y el ejercicio de la función administrativa.

En el evento de adquirirse bienes y/o servicios consistentes en Tecnologías de la Información y/o Softwares, los proveedores deberán dar cumplimiento a las disposiciones sobre ciberseguridad establecidas en el Decreto N° 273, de 13.SEP.022, del Ministerio del Interior y Seguridad Pública, esto es que compartan información sobre 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 estas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados, así como también, deberá dar cumplimiento a las Políticas de Seguridad de la información de la PDI, aprobadas por Orden General N° 2.812, de 03.NOV.023.

2 En cuanto a la **Propiedad de la Información**, se debe tener presente las condiciones de las Bases Administrativas publicadas en la plataforma www.mercadopublico.cl, las que se ajustan a los criterios definidos por la Dirección de Compras y Contratación Pública, en donde se establece. El proveedor no podrá utilizar la información indicada en el párrafo anterior, durante la ejecución del desafío, sin autorización escrita de la entidad mandante. Por tal motivo, una vez que el proveedor entregue dicha información a la entidad o al finalizar la relación contractual, deberá borrarla de sus registros lógicos y físicos.

En caso de que la entidad licitante entregue al adjudicatario licencias de software sólo podrán ser ejecutadas para la operación del servicio contratado y en ninguna circunstancia el proveedor adjudicado podrá utilizarlas para otros propósitos.

La entidad licitante será la titular de todos los datos, procedimientos que se generen en virtud de la ejecución de los servicios objeto de la presente licitación.

3 Prácticas normativas que debe cumplir como mínimo o que pueden afectar el diseño de la solución deben estar acorde a lo siguiente:

- Ley N° 21.663, denominada “Marco de Ciberseguridad”.
- Ley N° 19.628, denominada “Protección de la vida privada”.
- Decreto N° 273, que "Establece obligación de reportar incidentes de Ciberseguridad", de fecha 02.DIC.022.

4 El equipo innovador no tendrá acceso a realizar pruebas en entorno real (Etapa 3) de la Escena del Crimen por lo que deberá generar instructivos de trabajo respecto del uso de las tecnologías desarrolladas y capacitar sobre ellas a personal del Laboratorio de Criminalística para las pruebas que se requiera llevar a cabo en este tipo de ambientes.

5 A cada integrante de los equipos de trabajo se les solicitará certificado de antecedentes para el uso exclusivo de la Policía de Investigaciones de Chile.

6 Cabe señalar que, las empresas/instituciones, deben pasar por una revisión por parte de funcionarios policiales para acceder a las Instalaciones de la Policía de Investigaciones de Chile.

7 Al momento de ingresar a las dependencias de cualquier Unidad de la Policía de Investigaciones de Chile, se les deberá impartir una charla de seguridad en la cual se indicarán las restricciones y deberes.

7. Resumen del proyecto

En función de los aspectos detallados anteriormente, el desafío se organiza de la siguiente manera:

ítem	***Etapa 1***	***Etapa 2***	***Etapa 3***
N° proyectos a adjudicar	6	4	2
Descripción	Herramientas tecnológicas mínimamente invasivas capaces de identificar con exactitud igual o superior al 80% de sustancias biológicas como la sangre y/o residuos inorgánicos de un proceso de disparo, sin destruir ni alterar los materiales examinados durante el proceso de análisis. El plazo de ejecución de esta etapa es de seis meses.	Equipos portátiles mínimamente invasivos, de tamaño y peso apropiados para el transporte y operación en terreno, con autonomía de a lo menos cuatro horas, que sean resistentes al polvo y a la humedad capaces de realizar análisis en un amplio rango de temperatura, sin perder precisión ni sensibilidad y de ser estables frente a cambios rápidos de temperatura ambiente, resistentes a los golpes, con protocolos de verificación/calibración. El plazo de ejecución de esta etapa es de seis meses.	Equipos portátiles mínimamente invasivos, de tamaño y peso apropiados al transporte en terreno, con autonomía de hasta lo menos cuatro horas, que sean resistentes al polvo y a la humedad (IP 67 o mejor), capaces de realizar análisis en un amplio rango de temperatura, sin perder precisión ni sensibilidad y de ser estables frente a cambios rápidos de temperatura ambiente, resistentes a los golpes, con protocolos de verificación/calibración. El plazo de ejecución de esta etapa es de 12 meses.
Proyectos seleccionados que pasan a la siguiente Etapa	4	2	

8. Anexos

Se adjunta listado acotado de servicios periciales que ofrece el Laboratorio de Criminalística Central de la PDI, mencionando aquellos que tienen relación con las pericias que se aluden en la presente Guía.

1.- Sección Bioquímica y Biología Forense.

Servicio Pericial y reseña explicativa	***Levantamiento de evidencia biológica en Sitio del Suceso.*** Corresponde al levantamiento de evidencias de carácter biológico con interés criminalístico en el sitio del suceso, las que pueden ser de diversa categoría de acuerdo con el tipo de delito efectuado, como manchas atribuibles a restos biológicos, vestimentas, armas cortopunzantes, u otro objeto o soporte que pudiese presentar restos biológicos susceptibles de levantamiento. Asimismo, incluye la toma de muestra indubitada/referencia u otra no invasiva desde el cuerpo de un individuo vivo o muerto.

Requisitos Obligatorios	El levantamiento de evidencia biológica debe realizarse en el sitio del suceso, levantando el soporte en su totalidad o bien una muestra de él, de acuerdo a las condiciones presentes. En el caso de toma de muestras a individuos vivos, se requiere autorización voluntaria del donante o autorización voluntaria del tutor legal del donante, presencia de abogado defensor o una orden del Juzgado de Garantía, lo anterior de acuerdo a la normativa legal vigente respecto a las condiciones del donante (Código Procesal Penal Art. N° 197, mayor o menor de edad, interdicto, víctima o imputado, entre otros). La toma de muestra siempre debe cumplir lo estipulado en el Código Procesal Penal y en la Ley N° 20084 de Responsabilidad Penal Adolescente. Asimismo, se debe considerar lo estipulado en el Art. 11 y Art. 12 del Decreto 634 que Aprueba Reglamento de la Ley N° 19.970, que crea el Sistema Nacional de Registros de ADN, y lo estipulado en el numeral 6.2.1 de la Normativa Técnica para la Determinación de Huella Genética en Materia Forense bajo la Ley N° 19.970 y su Reglamento. Las evidencias biológicas levantadas podrían ser peritadas por esté Laboratorio o ser derivadas a otros, según requerimiento del ente solicitante. Debe ser realizado por un Profesional Perito de la Sección Bioquímica y Biología u otro Profesional competente.
Servicio Pericial y reseña explicativa	***Rastreo orientativo de vestigios sanguíneos latentes.*** Es la aplicación de un reactivo quimioluminiscente, que permite revelar de forma orientativa manchas de sangre latentes. Presentes en superficies en las cuales se presume que fueron lavadas, o donde las manchas son muy leves/ escasas, o las características propias de las evidencias hacen que las manchas no sean visibles.

Requisitos Obligatorios	Las superficies a peritar deben ser las que de acuerdo a la investigación criminal realizada por la Unidad solicitante, se presume que fueron lavadas, o donde las manchas son muy leves/ escasas, o las características propias de las evidencias hacen que las manchas no sean visibles. Se necesita que el lugar en estudio se encuentre oscurecido en su totalidad. Se puede realizar en el sitio del suceso y en el Laboratorio, toda vez que se cumpla el requisito anterior. Debe ser realizado por un Profesional Perito de la Sección Bioquímica y Biología o un Oficial Policial Profesional capacitado como Perito en Bioquímica y Biología.
Servicio Pericial y reseña explicativa	***Rastreo de vestigios seminales en delitos sexuales.*** Corresponde a la observación de forma orientativa mediante luz alterna a 450 nm con filtro anaranjado. La observación se realiza en superficies en las que se presume la presencia de manchas que podrían corresponder a restos de semen latente o no visible.
Requisitos Obligatorios	Se necesita que el lugar en estudio se encuentre oscurecido en su totalidad. Se puede realizar en el sitio del suceso y en el Laboratorio, toda vez que se cumpla el requisito anterior. Debe ser realizado por un Profesional Perito de la Sección Bioquímica y Biología o un Oficial Policial Profesional capacitado como Perito en Bioquímica y Biología.
Servicio Pericial y reseña explicativa	***Identificación de sangre de origen humano.*** Corresponde a una prueba de certeza para identificación de sangre humana.
Requisitos Obligatorios	Debe ser realizada considerando los rangos de temperatura óptimos para el ensayo a realizar, evitando temperaturas extremas. Debe ser realizado por un Profesional Perito de la Sección Bioquímica y Biología o un Oficial Policial Profesional capacitado como Perito en Bioquímica y Biología.

2.- Sección Balística.

Estudio Asociado a Vainillas y/o Proyectiles	
Servicio Pericial y reseña explicativa	***Identificación.*** Corresponde a establecer el calibre, sus inscripciones en el culote, el tipo de percusión que presenta, el tipo de proyectil al cual corresponde (artesanal o convencional), su rayado balístico y giro, señalando el tipo de arma de fuego que pudo haberla(s) disparado(s) y/o percutido(s), el presente estudio permitirá determinar el calibre y la cantidad mínima de armas de fuego que participaron en los hechos investigados.
Requisitos Obligatorios	Oficio petitorio señalando la respectiva solicitud de pericia Remitir la evidencia física, con su respectivo Formulario Único de Cadena de Custodia.

Estudio Asociado a Vainillas y/o Proyectiles	
Servicio Pericial y reseña explicativa	***Comparación microscópica. (dubitadas – testigos).*** Corresponde a establecer microscópicamente las coincidencias o diferencias de huellas de clase e individuales, las cuales son características y únicas de un arma de fuego, Establecerá la cantidad de armas de fuego que participaron en los hechos investigados o si el arma de fuego incautada (dubitada) tuvo participación en el delito. (*) Cabe señalar que se encuentra en etapa de estudio la comparación microscópica de proyectiles disparados en armas de fogueo adaptadas.
Requisitos Obligatorios	Oficio petitorio señalando la respectiva solicitud de pericia. Contar con al menos una (01) vainilla dubitada y un (01) arma de fuego, ambas de igual calibre, o en su defecto al menos dos (02) vainillas dubitadas del mismo calibre. Contar con al menos un (01) proyectil dubitado y un (01) arma de fuego, ambas de igual calibre, o en su defecto al menos dos (02) proyectiles dubitados del mismo calibre. Remitir la evidencia física, con su respectivo Formulario Único de Cadena de Custodia. La respuesta de este Servicio, comprende una ponderación inicial de al menos (3) días hábiles.

Estudio Asociado a Vainillas y/o Proyectiles	
Servicio Pericial y reseña explicativa	***Ingreso al Sistema IBIS de Vainillas y Proyectiles.*** Corresponde a dejar registro de las imágenes de las huellas de clase e individuales presentes en el culote de la vainilla y/o en el cuerpo del proyectil, las que serán correlacionadas con sus similares archivadas en la base de datos de dicho sistema. El estudio permitirá establecer si el arma de fuego ha participado en delitos ocurridos con anterioridad y que se encuentren archivados en la base de datos del Sistema. (*) Cabe señalar que es responsabilidad del operador IBIS, dar respuesta cuando no fue posible ingresar una evidencia.
Requisitos Obligatorios	Oficio petitorio señalando la respectiva solicitud de pericia. Que la vainilla haya participado en un proceso de disparo. Que el proyectil haya sido disparado por un arma de fuego convencional que cumpla con los parámetros de ingreso (con respecto a sus huellas). Remitir la evidencia física, con su respectivo Formulario Único de Cadena de Custodia.

Estudio Asociado a Prendas de Vestir	
Servicio Pericial y reseña explicativa	***Identificación de desgarraduras compatibles con el paso de un proyectil balístico (entrada y/o salida) y clasificación de la distancia de disparo (corta o larga distancia).*** Corresponde a una apreciación visual de la presencia de algún carácter constante o inconstante (anillo de limpieza, chamuscadura, halo carbonoso/tatuaje) sobre alguna de las desgarraduras presentes en prendas de vestir, que permitan eventualmente discriminar entre entrada o salida de proyectil, para establecer trayectoria de un disparo, que permitan clasificar la distancia de disparo como corta o larga distancia. En el caso de no poder clasificar la desgarradura como ingreso o salida de un proyectil, ésta se derivará a la Sección Microanálisis, quienes darán respuesta mediante la metodología propia de esa especialidad.

Requisitos Obligatorios	Oficio petitorio señalando la respectiva solicitud de pericia. Remitir la evidencia física, con su respectivo. Aportar en lo posible antecedentes médicos del lesionado. Formulario Único de Cadena de Custodia.
Estudio Asociado a Vehículos, Inmuebles y Otras Superficies	
Servicio Pericial y reseña explicativa	***Identificación, localización y descripción de un impacto balístico.*** Corresponde a rastrear la ubicación de los impactos con características compatibles con el paso de un proyectil, con el objeto de asociarlos a probables líneas de tiro, el estudio permitirá establecer cantidad de disparos efectuados en un sentido/dirección sobre el objeto de estudio, con la finalidad de precisar la posibilidad de un "intercambio de disparos".
Requisitos Obligatori	El oficial investigador debe estar siempre presente, quien deberá aportar los antecedentes preliminares del hecho, con la finalidad de interpretar la ubicación de los efectos de los disparos. Las pericias deberán ser realizadas con luz día. La inspección ocular de vehículos deberá ser en una zona segura. Se debe contar con una autorización verbal o escrita de por medio, en caso que haya que destruir partes de un domicilio y/o vehículo.

Estudio Asociado a Vehículos, **Inmuebles y Otras Superficies**	
Servicio Pericial y reseña explicativa	***Determinación de trayectoria y posición del tirador.*** Corresponde a determinar luego del análisis y estudio de los orificios y/o muescas presentes en el objeto de estudio, una relación y correspondencia entre estos, para establecer la trayectoria de los disparos y la posición de él o los tiradores.
Requisitos Obligatorios	Contar con la información obtenida de la identificación localización y descripción de él o los impacto(s) balístico(s). Que las pericias sean realizadas con luz día, lo que ayudará a tener una mejor descripción y a una mejor visión con respecto a las evidencias analizadas.

11.- Sección Microanálisis.

Servicio Pericial y Reseña Explicativa	***Determinación de desgarraduras de entrada y salida de proyectiles balísticos en prendas de vestir.*** Detectar partículas de residuos de disparos (GSR), así como, su distribución en los contornos de desgarraduras atribuibles al paso de proyectil balístico en prendas de vestir externas, a fin de establecer cuál de estas podría corresponder a la entrada y cual a la salida de un proyectil balístico y contribuir al esclarecimiento de la dinámica balística del hecho investigado, en particular, posición de la víctima respecto al tirador.

Requisitos Obligatorios	Este Servicio Pericial solo puede ser aplicado sobre prendas de vestir directamente expuestas al proceso de disparo y con a lo menos dos (02) desgarraduras balísticas (posibles entradas y salidas). Debido a limitaciones del equipamiento científico, no es posible analizar muestras de dimensiones superiores a 5 x 5 cm. En consecuencia, antes de solicitar la Pericia, evaluar la factibilidad que las especie sea cortada en esta Sección, a fin de extraer la desgarradura que será directamente examinada. Las prendas de vestir remitidas para Peritaje, deben ser manipuladas solo lo necesario para efectuar la descripción de la especie y elementos de interés, a fin de prevenir la pérdida de eventuales partículas de residuos de disparos (GSR). No cubrir las desgarraduras con cinta adhesiva. Remitir las prendas de vestir que serán examinadas en contenedores separados. Al embalar doblar cuidadosamente cada evidencia y disponer una hoja de papel blanco entre superficies que contengan desgarraduras, a fin de evitar transferencia cruzada de partículas de residuos de disparos, no asociadas al suceso balístico. El Oficial Policial deberá proporcionar la mayor cantidad de antecedentes relacionados con la dinámica de los hechos, con la finalidad de facilitar la interpretación de los resultados obtenidos. Principalmente, si la prenda de vestir era usada por el revés o por el derecho al momento de producirse las lesiones en la víctima.

APRUEBA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023-2028

Núm. 164.- Santiago, 16 de junio de 2023.

Vistos:

Lo dispuesto en los artículos 24, 32 Nº 6 y 35 del decreto supremo Nº 100, de 2005, del Ministerio Secretaría General de Presidencia, que fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile; en el decreto con fuerza de ley 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 la ley Nº 19.880 de bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado; 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 el decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad y su modificación mediante el decreto supremo Nº 579, de 2020, de la misma cartera de Estado; en el instructivo presidencial Nº 1, de 27 de abril de 2017, que Instruye Implementación de la Política Nacional sobre Ciberseguridad; en el acuerdo del Comité Interministerial sobre Ciberseguridad, tomado en sesión de fecha 25 de mayo de 2023, que aprueba la propuesta de Política Nacional de Ciberseguridad para el período 2023-2028; y la resolución Nº 7, del año 2019, de la Contraloría General de la República;

Considerando:

1º Que, conforme a lo dispuesto en el artículo 1º de la ley Nº 20.502, corresponde al Ministerio del Interior y Seguridad Pública concentrar las decisiones políticas, así como coordinar, evaluar y controlar la ejecución de planes y programas en materia de seguridad pública, para lo cual puede solicitar la colaboración de los demás organismos que integran la Administración del Estado, propendiendo a la unidad de acción.

2º Que, durante los últimos años las tecnologías de información y comunicaciones (TIC) han tomado un rol fundamental en la manera de desenvolvernos como sociedad. La consolidación de este mundo digital ha traído múltiples oportunidades efectivas de bienestar y crecimiento tanto social como económico; sin embargo, este tejido digital es frágil porque implica inevitablemente una serie de riesgos y amenazas para la seguridad de las personas.

3º Que, nuestro país enfrenta desafíos importantes en la materia, teniendo un nivel medio de madurez en comparación al resto del escenario internacional, conforme lo indica el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomunicaciones. En el Índice Mundial de Ciberseguridad del año 2020, Chile se encuentra en el lugar 74 a nivel mundial, y en el 7º lugar en América (debajo de Estados Unidos, Canadá, Brasil, México, Uruguay y República Dominicana). En este índice, Chile se destaca por su avance en medidas legales, medidas organizacionales y de

cooperación; sin embargo, se queda atrás en el ámbito técnico. En el Índice Nacional de Ciberseguridad, desarrollado por Estonia y actualizado de forma continua, Chile se encuentra al año 2023 en el lugar 53 entre 175 países, y en el 6º lugar en Latinoamérica y el Caribe, debajo de República Dominicana, Argentina, Paraguay, Perú y Uruguay. En este ranking, que consta de 12 áreas distintas, Chile se destaca en desarrollo de políticas de ciberseguridad, lucha contra el cibercrimen y operaciones militares; pero se queda atrás en protección de servicios esenciales, protección de servicios digitales, gestión de crisis y protección de datos personales.

4º Que, el programa de gobierno establece, en materia de derechos digitales, la protección de la información y ciberseguridad, y la implementación robusta de la Política Nacional de Ciberseguridad (en adelante "Política" o PNCS), que es el instrumento de planificación del Estado de Chile en materia de ciberseguridad y que tiene por objeto contar con un ciberespacio libre, abierto, seguro y resiliente, otorgando, a su vez, especial protección a mujeres, niñas, niños, adolescentes, adultos mayores y diversidades sexogenéricas.

5º Que, a través del decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública, se creó el Comité Interministerial sobre Ciberseguridad, a quien se le encomendó la misión de proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia.

6º Que, con fecha 25 de mayo de 2023, en el Palacio La Moneda, comuna de Santiago, Región Metropolitana, se llevó a cabo la sesión del Comité Interministerial sobre Ciberseguridad, en la que se aprobó la propuesta de Política Nacional de Ciberseguridad 2023-2028, por la unanimidad de los miembros presentes con derecho a voto, de conformidad con lo dispuesto en el artículo sexto del decreto supremo Nº 533, de 2015, del Ministerio del Interior y Seguridad Pública.

7º Que, la referida propuesta de Política Nacional de Ciberseguridad 2023-2028, es el resultado de un proceso participativo que consideró la opinión de numerosos actores del mundo público y privado, quienes a través de audiencias públicas y consultas ciudadanas expresaron sus preocupaciones y visiones sobre los problemas y desafíos que conlleva la vida digital. Asimismo, para la construcción de la Política se siguieron las recomendaciones de la Guía para desarrollar una estrategia nacional de ciberseguridad, de la Unión Internacional de Telecomunicaciones(1); se observó la experiencia de países con un nivel similar al nuestro en la materia, como Argentina, Uruguay y República Dominicana, y de otros más avanzados, como Israel, Reino Unido y Estados Unidos; se consultaron diversas publicaciones internacionales y se realizó una evaluación del proceso de implementación de las medidas de la primera Política Nacional de Ciberseguridad.

Decreto:

Artículo único.- Apruébase la Política Nacional de Ciberseguridad, para el período 2023-2028, cuyo texto es el siguiente:

POLÍTICA NACIONAL DE CIBERSEGURIDAD

1. Introducción

Las tecnologías de información y comunicaciones (TIC) juegan un papel fundamental en las actividades diarias y en el bienestar de las personas, en la generación de riqueza para los países, en la provisión de servicios básicos para las sociedades, y en la seguridad y soberanía de las naciones. Tanto la cantidad y variedad de usos que damos a las TIC como el número de personas con acceso han aumentado de forma acelerada en los últimos 20 años, generando nuevas oportunidades de desarrollo social y crecimiento económico. Sin embargo, la tecnología es inherentemente vulnerable. La mayor parte de las TIC no fueron diseñadas pensando en la seguridad de la información, posibilitando que diversos actores sean capaces de dañar a personas y organizaciones a través de estas tecnologías.

En abril de 2017, la entonces presidenta Michelle Bachelet lanzó la primera Política Nacional de Ciberseguridad de Chile, que contenía cinco objetivos de política pública en materia de ciberseguridad, y una serie de 41 medidas a ser implementadas entre los años 2018 y 2022. La Política fue confirmada por el gobierno del presidente Sebastián Piñera, progresando en el diseño de la institucionalidad y el fortalecimiento del marco regulatorio, y permitiendo al país avanzar de manera decidida en los retos que enfrentamos. Los desafíos se han diversificado y complejizado, y el escenario global cambia de forma acelerada, lo que hace necesario robustecer con celeridad las mismas áreas de protección consideradas en la primera política, y generar nuevas capacidades para adaptarnos a circunstancias distintas de las que se previeron hace cinco años.

_____

(1) Guide to Developing a National Cybersecurity Strategy, 2nd edition 2021.

El gobierno del presidente Gabriel Boric ha continuado con el proceso de implementación de la Política Nacional de Ciberseguridad 2017-2022 y ha impulsado la discusión del proyecto de ley marco sobre ciberseguridad, poniendo especial énfasis en la protección y defensa de los derechos de las personas, la equidad de género, y la profundización de la democracia. Se ha procurado brindar protección a aquellos grupos que se ven mayoritariamente afectados por la violencia digital y los ciberdelitos, teniendo en consideración que las amenazas del ciberespacio no impactan a todos por igual, siendo las principales víctimas las mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas.

Para incrementar nuestro nivel de madurez en ciberseguridad, necesitamos contar con un ciberespacio libre, abierto, seguro y resiliente, tal como fue planteado en la primera Política Nacional de Ciberseguridad, que constituyó una política de Estado y, como tal, debe ser renovada.

La presente Política es el resultado de la participación de numerosos actores del mundo público y privado, que a través de audiencias públicas expresaron sus preocupaciones y visiones sobre los problemas y desafíos que conlleva la vida digital. La sociedad civil tuvo un rol fundamental en su elaboración a través de dos consultas ciudadanas, una previa y otra posterior a su redacción. Para su elaboración se siguieron las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT)(2), se observó la experiencia de países similares y más avanzados, se consultaron diversas publicaciones internacionales (3) y se realizó una evaluación del proceso de implementación de las medidas de la primera Política. Esta segunda política representa

tanto una continuación de los esfuerzos de la primera, como una readecuación del foco para los próximos años producto de la revisión de los cambios sucedidos desde entonces.

1.1. ¿Por qué necesitamos una Política Nacional de Ciberseguridad?

El siglo en curso probablemente verá más cambios que toda la historia de la humanidad, tanto en términos culturales como políticos y económicos. El calentamiento global acelera el cambio climático, acentuando climas extremos y aumentando la frecuencia y duración de eventos como sequías, inundaciones, tornados e incendios forestales. La disponibilidad de agua ha disminuido, lo que afecta la agricultura y disminuye nuestra capacidad para generar alimentos(4). Todos estos cambios ya están afectando a nuestro país, y se espera que se aceleren durante este siglo.

La pandemia de SARS CoV-2 (COVID-19) ha producido, a abril de 2023, poco más de 6,8 millones de muertes en el mundo(5) y más de 52 mil muertes confirmadas en nuestro país (6). Además del enorme costo social en términos de salud pública, la pandemia aceleró múltiples procesos de transformación digital. La productividad de la mayor parte de las sociedades se ha visto mermada de forma considerable durante varios años, lo que contribuye a una recesión económica en ciernes o declarada en decenas de países. Tal como ocurrió con la epidemia mundial de gripe de 1918, los efectos de la actual pandemia tardarán muchos años en desaparecer.

Finalmente, la inestabilidad política y económica que ha generado la guerra en Europa del Este nos pone en un escenario que no veíamos desde la segunda guerra mundial. Antes del conflicto, Ucrania producía el 10% del trigo, el 15% del maíz y el 13% de la cebada del mundo(7). La escasez de grano generó durante varios meses aumentos de precios y ha contribuido al aumento de la inflación en muchas economías.

---

(2) Guide to Developing a National Cybersecurity Strategy, 2nd edition 2021.

(3) Como las guías y manuales del Cooperative Cyber Defence Centre of Excellence de la OTAN; la National Cyber Security Strategies de ENISA; el Modelo de Madurez de Capacidades de Ciberseguridad para Naciones de la Universidad de Oxford; y el Í ndice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones.

(4) IPCC, 2022: Summary for Policymakers [H.-O. Pörtner, D.C. Roberts, E.S. Poloczanska, K. Mintenbeck, M. Tignor, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem (eds.)]. In: Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [H.-O. Pörtner, D.C. Roberts, M. Tignor, E.S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, B. Rama (eds.)]. Cambridge University Press, Cambridge, UK and New York, NY, USA, pp. 3-33, doi:10.1017/9781009325844.001.

(5) https://www.worldometers.info/coronavirus/.

(6) https://www.gob.cl/pasoapaso/cifrasoficiales/.

(7) https://www.dw.com/en/five-facts-on-grain-and-the-war-in-ukraine/a-62601467.

Todo lo anterior es relevante para nuestro país, pero ¿qué relación tiene con la ciberseguridad?

La ciberseguridad no es un fin en sí mismo. La ciberseguridad es una condición que, de existir, permite el uso pleno de Internet y de la web, herramientas habilitadoras y

potenciadoras de las actividades humanas. Todos nuestros esfuerzos para enfrentar desafíos como el cambio climático y la pandemia de COVID-19, y para devolver la paz y la estabilidad política y económica al mundo, pueden verse facilitados o entorpecidos por la presencia o ausencia de las herramientas de comunicación provistas a través de las redes y sistemas informáticos.

En diciembre de 2003, la World Summit on the Information Society, formada bajo el auspicio de la Organización de las Naciones Unidas (ONU), publicó una declaración de principios de la Sociedad de la Información luego de largas negociaciones con organizaciones privadas, públicas y representantes de la sociedad civil de todos los países congregados(8). En el punto 4 de la declaración se afirma que "que todo individuo tiene derecho a la libertad de opinión y de expresión, que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social." (9). Es la satisfacción de esta necesidad humana básica y derecho humano fundamental la que hacemos posible a través de la ciberseguridad. Todo Estado tiene hoy el deber de generar las condiciones para permitirle a cada persona ejercer este derecho.

Veinte años después, en enero de 2023, el World Economic Forum publicó un reporte(10) donde presentan una serie de problemas sobre ciberseguridad, desde la perspectiva de expertos y líderes de negocio alrededor del mundo, destacándose los siguientes:

. La inestabilidad geopolítica global ha convencido a líderes y expertos por igual de la importancia de la gestión de los riesgos de ciberseguridad. 91% de los participantes del estudio creen que un incidente catastrófico de ciberseguridad es relativamente probable dentro de los próximos dos años.

. 43% de los líderes piensa que es probable que su organización sea atacada a través del ciberespacio dentro de los próximos dos años.

. Las preocupaciones sobre ciberseguridad y protección de datos personales están crecientemente influyendo en cómo y dónde operan los negocios. El nivel de ciberseguridad que cada país es capaz de mantener está siendo considerado por inversionistas para tomar decisiones sobre dónde invertir.

. La naturaleza de las amenazas en el ciberespacio ha cambiado. Tanto líderes de negocio como expertos en ciberseguridad creen que los atacantes se están concentrando en dañar los procesos de negocio, y en arruinar la reputación de las organizaciones.

Nuestra economía, la mayor parte del comercio internacional, nuestras actividades de ocio, los medios de comunicación masivos, las interacciones sociales y políticas, y la mantención y difusión de nuestra cultura: todas dependen fuertemente del acceso a Internet y a los medios y aplicaciones que posibilita. Es por eso que la primera versión de la Política Nacional de Ciberseguridad (2017-2022) fijó como objetivo para el 2022 el contar con un ciberespacio libre, abierto, seguro y resiliente; por la misma razón, la nueva Política Nacional de Ciberseguridad (2023-2028) perseguirá el mismo objetivo.

1.2. Los desafíos en ciberseguridad en nuestro país

Chile tiene un nivel medio de madurez en ciberseguridad en el escenario internacional. En el Índice Mundial de Ciberseguridad de 2020(11), Chile se encontraba en el lugar 74 a nivel mundial, y en el 7º lugar en América (debajo de Estados Unidos, Canadá, Brasil, México, Uruguay y República Dominicana). En este índice, Chile se destaca por su avance en medidas legales, medidas organizacionales y de cooperación; sin embargo, se queda atrás en las medidas técnicas.

_____

(8) https://en.wikipedia.org/wiki/Right_to_Internet_access.

(9) httos://www.itu.int/net/wsis/docs/geneva/official/dop.html.

(10) Global Cybersecurity Outlook 2023, Insight Report, Enero 2023. World Economic Forum. En colaboración con Accenture. Ver https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.

(11) Global Cybersecurity Index, de la International Telecommunication Union, es un ránking que mide "el grado de compromiso" de los 193 países miembros de la ITU con cinco pilares: jurídico, técnico, organizacional, de capacitación y de cooperación. Ver https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity -index.aspx.

En el Índice Nacional de Ciberseguridad(12), desarrollado por Estonia y actualizado de forma continua, Chile se encuentra, al año 2023, en el lugar 53 entre 175 países, y en el 6º lugar en Latinoamérica y el Caribe, debajo de República Dominicana, Argentina, Paraguay, Perú y Uruguay. En este ránking, que consta de 12 áreas distintas, Chile se destaca en desarrollo de políticas de ciberseguridad; lucha contra el cibercrimen, y operaciones militares; pero se queda atrás en protección de servicios esenciales; protección de servicios digitales, gestión de crisis y protección de datos personales.

Los principales problemas que enfrentamos hoy en materia de ciberseguridad en nuestro país son:

1. La insuficiente resiliencia de nuestras organizaciones e infraestructura. Brechas de seguridad recientes en el país nos confirman la necesidad de fortalecer la protección de nuestra infraestructura de redes y sistemas; además de mejorar el entrenamiento y formación de los funcionarios públicos, así como de todas las personas en organizaciones que lo requieran. Para esto, es necesario monitorear nuestro ciberespacio de forma efectiva, especialmente la infraestructura de redes del sector público, de los servicios esenciales y los operadores de importancia vital.

2. La falta de cultura de las organizaciones y de las personas sobre la importancia de la ciberseguridad. Esto, junto a la falta de conocimiento, lleva a que tanto las organizaciones como las personas no tomen medidas suficientes de protección en el ciberespacio. El desafío para el Estado es entregar alfabetización básica en ciberseguridad y generar conciencia de su importancia en cada persona, desde la segunda infancia hasta los adultos mayores, tanto en la educación básica y media, como en las organizaciones privadas, el sector público y la sociedad civil. Para abordar este desafío el Estado velará especialmente por los territorios más apartados.

3. La falta de especialistas en ciberseguridad. Se estima que en Chile faltan alrededor de 28.000 especialistas en ciberseguridad para satisfacer las necesidades tanto del sector público como privado, y que en carreras relacionadas específicamente a la ciberseguridad, solo el 10% son cupos femeninos, cifra que se condice con el 15% de

participación de mujeres en los puestos laborales de ciberseguridad que existen en el país(13). La ausencia de mujeres en el mundo laboral y en las carreras relacionadas con computación e informática, tanto en centros de formación técnica como en universidades e institutos profesionales, encuentra su explicación en distintas condiciones sociales que desincentivan su participación, y no en una falta de interés de las mujeres en el área. Es necesario que el Estado genere las condiciones para disminuir estas brechas, incentivando que una mayor cantidad de personas escoja estudiar carreras relacionadas con la ciberseguridad y promoviendo un aumento de la participación femenina en el sector, especialmente considerando que las mujeres representan un 52,4% de la población chilena.

4. La falta de sofisticación de nuestra demanda por ciberseguridad. Se estima que la industria de ciberseguridad en nuestro país realiza ventas anuales por alrededor de $350 millones de dólares, lo que representa un 0.11% del PIB de Chile(14). La ciberseguridad es un área económica intensiva en capacidades, que a futuro podría representar una parte creciente de nuestro producto interno bruto, ayudar a posicionar a nuestro país en el escenario latinoamericano, e incluso fortalecer la confianza en nuestra economía, vista desde el exterior. Sin embargo, para que esto suceda, es necesario tener una demanda más amplia y sofisticada.

5. El aumento de delitos en el ciberespacio. De acuerdo con la encuesta nacional urbana de seguridad ciudadana, durante los últimos años la tasa de denuncia de los delitos informáticos se ha incrementado progresivamente desde un 6,6% en 2017 a un 10,1% en 2021(15). Este tipo de delitos pone en riesgo la seguridad y la confianza de las personas en el ciberespacio y es un fenómeno que debe abordarse desde una perspectiva preventiva y sancionatoria.

---

(12) National Cybersecurity Index (NCSI). Ver https://ncsi.ega.ee.

(13) Estudio #2: Estimación de la brecha de expertos en ciberseguridad en Chile. Coordinación Nacional de Ciberseguridad, enero de 2023. Disponible en https://bit.ly/cnc-eb02

(14) Estudio #1: RFI de la industria de ciberseguridad en Chile. Coordinación Nacional de Ciberseguridad, diciembre de 2022. Disponible en https://bit.ly/cnc-eb01

(15) Disponible en https://www.ine.gob.cl/estadisticas/sociales/seguridad-publica-y-justicia/seguridad-ciudadana

Nuestro país se ve afectado sin ninguna duda por las tendencias globales, pero además tiene problemas específicos. Hay grupos de atacantes que han estado muy activos en Latinoamérica y se han autoproclamado responsables de grandes filtraciones de datos que ocurrieron en 2022 y 2023. La cantidad de incidentes que se registran en la Red de Conectividad del Estado (la red de datos que presta conectividad a una parte importante del sector público) confirma que una de las preocupaciones fundamentales de los próximos meses debe ser el fortalecimiento de la infraestructura pública, así como la formación y entrenamiento del personal público, además de un robustecimiento de los servicios esenciales y operadores de importancia vital.

1.3. Los cinco objetivos de la Política Nacional de Ciberseguridad

Para enfrentar los problemas y los desafíos anteriores, la nueva Política Nacional de Ciberseguridad contiene cinco objetivos fundamentales:

1. Infraestructura resiliente: El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos.

2. Derechos de las personas: El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas necesarias para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente.

3. Cultura de ciberseguridad: Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas.

4. Coordinación nacional e internacional: El Estado creará una gobernanza pública para coordinar las acciones necesarias en ciberseguridad. Los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en esta área.

En el ámbito internacional, el Estado se coordinará con países, organismos, instituciones y otros actores internacionales para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio.

5. Fomento a la industria y la investigación científica: El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Para ello, fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país.

La elección de los objetivos anteriores no es aleatoria: es posible establecer una relación entre ellos y las dimensiones definidas en al menos dos modelos internacionales en ciberseguridad(16).

Adicionalmente, la política incluye algunas dimensiones transversales con las que se busca proteger y promover la protección de los derechos de las personas y sus familias en Internet:

1. Equidad de género: todas las iniciativas considerarán de manera preferente a las mujeres, tanto para aumentar su seguridad en el entorno digital, al ser ellas las principales víctimas de violencia digital, como para mejorar su inclusión, mediante acciones positivas dirigidas a corregir las inequidades existentes en nuestra sociedad. Ello, pues a pesar de representar a más del 50% de la población chilena, su participación en los puestos laborales de ciberseguridad que existen en el país apenas alcanza el 15%.

2. Protección a la infancia: todas las iniciativas deben considerar protección preferente a niñas, niños y adolescentes.

3. Protección al adulto mayor: todas las iniciativas deben considerar protección preferente a adultos mayores.

4. Protección del medio ambiente: todas las iniciativas deben minimizar su impacto negativo sobre el medio ambiente.

_____

(16) El Modelo de Madurez de la Capacidad de Ciberseguridad (CMM) del Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford (https://gcscc.ox.ac.uk/the-cmm), y también el Indice de Ciberseguridad Global (ICG) publicado por la Unión Internacional de Telecomunicaciones en 2020 (https://www.itu.intidms_pub/itu-d/opb/str/D-STR-GC1.01-2021-PDF-S.pdf).

A diferencia de la versión anterior de la Política, el Plan de Acción se publicará de forma separada pues contiene medidas que se implementarán a corto plazo, mientras que la Política es un instrumento de largo plazo. El propósito es permitir revisar el avance, proponer cambios y mejoras, y enmendar oportunamente el rumbo en caso necesario durante la implementación de la Política en vez de sólo al final de su vigencia. Cada medida tendrá una institución responsable de conducir los esfuerzos para lograr su implementación, y reportará al Comité Interministerial sobre Ciberseguridad de forma periódica los avances observados o la falta de ellos. Cada medida estará asociada a resultados claros y medibles, y a plazos de consecución.

El Comité Interministerial sobre Ciberseguridad sugerirá alternativas de seguimiento e implementación de la Política, y asesorará el cumplimiento de sus medidas para conseguir los objetivos de política pública contenidos en este documento.

El Gobierno podrá utilizar una serie amplia de medidas políticas, económicas, estratégicas y sociales para lograr la implementación de las medidas, y para generar las condiciones para hacer surgir un ecosistema de ciberseguridad en el país, en conformidad con las políticas delineadas en este documento.

El Estado incentivará progresivamente la investigación y desarrollo aplicados en ciberseguridad, y estimulará la inversión privada en el área, en conjunto con las instituciones de educación superior y centros de investigación nacionales. La investigación científica aplicada es un deber ineludible y necesario del Estado, para generar conocimiento que permita aumentar la eficiencia de los factores productivos, generar valor agregado sobre la mera extracción de materias primas, y proveer servicios que le entreguen al país ventajas en el contexto comercial internacional. La investigación en ciberseguridad es una condición necesaria para generar un ecosistema de ciberseguridad en nuestro país, y para cumplir con los objetivos de política pública contenidos en este documento.

1.4. Relación con otros objetivos nacionales

. Política de ciberdefensa

Nuestro país tiene una Política de Ciberdefensa vigente, publicada en marzo de 2018, aprobada mediante el decreto supremo Nº 3, de 2017, del Ministerio de Defensa Nacional. En ella se establecen dos prioridades:

1. La cooperación internacional: Chile colaborará con otros países y promoverá medidas de transparencia y confianza en instancias como la ONU, la OEA, UNASUR, y otros, en coordinación con el Ministerio de Relaciones Exteriores.

2. El desarrollo de capacidades: El sector de la Defensa Nacional desarrollará líneas de carrera en cada rama de las Fuerzas Armadas. Para ello, creará un Comando Conjunto

de Ciberdefensa y un Centro de Respuesta a Incidentes de Seguridad Informática de Defensa (CSIRT de la Defensa Nacional).

Es importante mencionar que la ciberdefensa es fundamental para el cumplimiento de los objetivos nacionales de ciberseguridad, por lo que se debe propender a fortalecer las capacidades del país para enfrentar las ciberamenazas que puedan atentar contra la seguridad del país y poner en riesgo la soberanía nacional.

Adicionalmente, la Política de Ciberdefensa establece un principio de equivalencia: Chile podrá considerar ciberataques masivos sobre sus habitantes, su infraestructura o sus intereses como un ataque armado, en el contexto del Artículo 51 de la Carta de las Naciones Unidas. Este principio pone la infraestructura de comunicaciones de Internet al mismo nivel que la infraestructura considerada estratégica y vital para el país, como la red de transporte y la red de centros de salud, entre otros. La presente Política está en armonía con la Política de Ciberdefensa, y especifica objetivos de política pública que están en plena concordancia con los objetivos y prioridades de ese instrumento de planificación, particularmente en lo que respecta al objetivo de Coordinación Nacional e Internacional.

De igual forma, el sector de la Defensa Nacional realizará la reorganización orgánica que sea necesaria para el cumplimiento de sus funciones en el ciberespacio.

. Política Nacional de Inteligencia Artificial

Nuestro país posee también una Política Nacional de Inteligencia Artificial, publicada en diciembre de 2021 aprobada mediante el decreto supremo Nº20, de 2021, del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. En ella se establecen cuatro principios transversales: Inteligencia Artificial (o IA) centrada en el bienestar de las personas, IA para el desarrollo sostenible, IA inclusiva, e IA globalizada y en evolución. En la Política se establecen además tres ejes:

1. Factores habilitantes, como el desarrollo de talentos, la infraestructura tecnológica y la promoción y fomento del uso masivo de datos para la toma de decisiones.

2. Desarrollo y adopción, donde se incluyen la investigación básica y aplicada, la transferencia tecnológica, innovación, emprendimiento, mejoramiento de servicios públicos, y desarrollo económico basado en tecnología, entre otros.

3. Ética, aspectos normativos y efectos socioeconómicos, donde se considera un conjunto amplio y heterogéneo de tópicos y áreas de discusión y reflexión, entre los cuales se encuentra: ciberseguridad, ciberdefensa, género, etc.

La presente política está en plena concordancia con los objetivos y ejes planteados en la Política Nacional de Inteligencia Artificial, particularmente en el primer eje sobre la formación y desarrollo de talentos, y la capacitación y concientización de las personas; lo planteado en el segundo eje sobre investigación aplicada, transferencia tecnológica, emprendimiento y mejora de los servicios públicos; y respecto al tercero, en referencia a la promoción de sistemas tecnológicos seguros y robustecimiento de la institucionalidad en ciberseguridad.

. Política Nacional contra el Crimen Organizado

Finalmente, nuestro país cuenta con una Política Nacional contra el Crimen Organizado, aprobada mediante decreto supremo Nº 369, de 2022, del Ministerio del Interior y Seguridad Pública, con el propósito de disminuir la actividad delictiva de las

organizaciones criminales que operan en Chile, a través de la acción planificada y coordinada de las instituciones del Estado. Esta política tiene tres objetivos fundamentales: desarticular bandas y organizaciones criminales, implementar medidas específicas para controlar diversos delitos y fortalecer la coordinación interinstitucional a través de la consolidación de un ecosistema de seguridad pública. El segundo de los objetivos anteriores menciona explícitamente el cibercrimen como una de las formas de delito a combatir.

Dentro de las medidas propuestas por la Política anterior está la elaboración de una nueva Política Nacional de Ciberseguridad para el período 2023-2028, la tramitación de un proyecto de ley marco sobre Ciberseguridad e Infraestructura Crítica, y desarrollar estrategias de prevención y educación digital.

La presente Política está en plena concordancia con la Política Nacional contra el Crimen Organizado, específicamente en lo que se refiere a la prevención de la comisión de delitos informáticos, a la generación de una cultura de ciberseguridad en nuestro país, y a la coordinación entre instituciones de gobierno e instituciones privadas. Una de las motivaciones de esta coordinación es el intercambio de información y la colaboración para evitar y combatir de mejor forma el cibercrimen.

2. Objetivos de la Política Nacional de Ciberseguridad 2023-2028

2.1. Infraestructura resiliente

El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos. Para ello, es necesario avanzar en el fortalecimiento de los elementos técnicos, físicos y lógicos de nuestro ciberespacio, incluida nuestra creciente red de dispositivos conectados a Internet (Internet de las Cosas).

Para avanzar en este objetivo, es necesario:

1. Impulsar la tramitación del proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información, que crea la Agencia Nacional de Ciberseguridad, que opere como el órgano rector de la ciberseguridad en Chile, con facultades normativas, fiscalizadoras y sancionatorias, que ayude a incrementar el nivel de madurez institucional en ciberseguridad, tanto en el sector público como privado.

2. Crear el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), para atender las necesidades y requerimientos de protección y recuperación ante incidentes en el sector público y privado que afecten a organismos considerados de importancia vital.

3. Fortalecer la resiliencia de nuestros servicios esenciales frente a incidentes de ciberseguridad. Las instituciones públicas y privadas que operen servicios considerados vitales deben mejorar su nivel de madurez en ciberseguridad y su capacidad de sobreponerse a brechas y ataques. El Estado entregará recomendaciones y lineamientos básicos que permita a las instituciones protegerse frente a los ataques más frecuentes o de mayor impacto.

4. Robustecer la resiliencia física de la red en Chile. El Estado, conforme a lo dispuesto en los cuerpos legales y reglamentarios pertinentes, promoverá en coordinación con el

sector privado la priorización de la conexión de lugares previamente no conectados, o donde no exista redundancia de conexiones con al menos otros dos lugares.

5. Fortalecer el análisis de la información de red en el ciberespacio nacional, a través de la inversión en investigación científica aplicada en conjunto con el sector académico y la industria nacional, para colocar a Chile a la vanguardia en Latinoamérica en la generación de conocimiento y desarrollo de tecnología en ciberseguridad.

2.2. Derechos de las personas

El Estado resguardará y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad pública en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas suficientes para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente, otorgando especial protección a mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas, Todas las personas deberían poder hacer uso de Internet para comunicarse, trabajar, estudiar, y desarrollarse en lo personal, familiar y social en un entorno de equidad, inclusión, justicia y protección a la diversidad.

Para avanzar en este objetivo, es necesario:

1. Fortalecer el marco normativo sobre ciberseguridad y protección de datos personales, a través de la aprobación e implementación de la ley marco de ciberseguridad y la ley sobre protección de datos personales.

2. Generar instancias de capacitación para todos los funcionarios públicos en hábitos y medidas básicas de seguridad digital, que les permitan proteger la información de ciudadanos y ciudadanas que les es confiada y que administran a través de redes y sistemas computacionales.

3. Prevenir la comisión de delitos informáticos, con énfasis en aquellos que afectan a mujeres, niñas, niños y adolescentes, adultos mayores y disidencias sexogenéricas, debido a su mayor vulnerabilidad en el ciberespacio.

4. Identificar y corregir inequidades en el acceso y uso del ciberespacio producidas por la falta de conocimiento de seguridad digital en personas y grupos sociales en situaciones de mayor vulnerabilidad frente a incidentes.

2.3. Cultura de Ciberseguridad

Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas. La protección de la sociedad va en directa relación con la capacidad que tenga cada persona de protegerse. Se requiere generar nociones y prácticas de ciberhigiene en la población, de forma que cada uno sea capaz de cuidar por sí mismo su identidad digital y su información.

Para avanzar en este objetivo, es necesario:

1. Diseñar e implementar un plan de concientización nacional sobre ciberseguridad y privacidad, para que todas las personas que usen un computador o teléfono inteligente, independientemente de la región del país en que se encuentren, adquieran nociones y prácticas de ciberhigiene. Este programa se enfocará especialmente en mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas, así como en personas que vivan fuera de la Región Metropolitana y en otros grupos que podrían estar en

desventaja frente al resto de la sociedad en términos de conocimiento sobre ciberseguridad; y en micro y pequeñas empresas.

2. Generar e implementar un plan matriz de introducción y mejora de la educación en ciberhigiene y ciberseguridad para el sistema de enseñanza básica, media científico-humanista y media técnico-profesional. En particular, este plan considerará evaluar la generación de especialidades para la educación media técnico-profesional y la incorporación de materias de ciberhigiene y ciberseguridad a especialidades afines a lo largo del país.

3. Fomentar una cultura de evaluación y gestión del riesgo, tanto en organizaciones públicas como privadas, que nos permita prepararnos frente a incidentes y desastres que puedan afectar gravemente a las personas de nuestro país, su bienestar, su salud, sus derechos, su identidad, sus bienes o la posibilidad de desarrollarse plenamente a través de Internet.

4. Promover la investigación científica aplicada en ciberseguridad para resolver problemas que nuestro país enfrentará en los próximos años debido al uso e implementación intensiva de tecnologías con aplicaciones insospechadas. Nuestro país no puede ser simplemente un consumidor pasivo de tecnologías desarrolladas en el exterior. Es responsabilidad del Estado generar las condiciones para resolver problemas técnicos complejos que requieran de investigación científica y que surjan de las necesidades y requerimientos de protección de nuestras personas y organizaciones.

2.4. Coordinación nacional e internacional

Para aprovechar de manera eficiente y eficaz los recursos disponibles, resulta indispensable la acción coordinada e intencionada hacia la consecución de los objetivos de política pública. Los organismos públicos y privados promoverán instancias de cooperación con el resto del sector público y de la industria, y con la futura autoridad nacional de ciberseguridad, con especial énfasis en la comunicación y difusión de los esfuerzos que se realicen en ciberseguridad, a fin de evitar la duplicación de trabajo y la pérdida de recursos. En el ámbito internacional, el Estado se coordinará y trabajará con países, organismos, instituciones y otros actores internacionales, para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio, y contribuir de esa forma a fortalecer su liderazgo regional en ciberseguridad.

Para avanzar en este objetivo, es necesario:

1. Generar instancias de colaboración y cooperación entre organizaciones públicas y privadas en diversos ámbitos, como educación, infraestructura, protección de derechos, fomento a la industria, y otras áreas relacionadas con la ciberseguridad que puedan ser de interés del país, con el propósito de dar a conocer las iniciativas en desarrollo y coordinarlas adecuadamente.

2. Establecer relaciones de cooperación con instituciones de ciberseguridad de países avanzados en el área para aprender sobre sus experiencias y traer experiencia relevante a la implementación de iniciativas o proyectos en ciberseguridad. Para ello, se desarrollará una estrategia de cooperación internacional mediante la cual se establezcan prioridades y líneas de acción específicas.

3. Aumentar la participación en instancias multilaterales, particularmente en el ámbito de las Naciones Unidas y la Organización de los Estados Americanos, como también en iniciativas de múltiples partes interesadas. De la misma forma, se potenciará el trabajo y colaboración en el marco del Convenio de Budapest.

4, Promover activamente la ciberdiplomacia, incentivando a nivel regional y global la discusión respecto a la aplicación de normas, derecho internacional, y medidas de fomento de la confianza en el ciberespacio, y el desarrollo de acuerdos bilaterales que refuercen la cooperación en ciberseguridad, y el respeto de los derechos humanos en el ciberespacio.

5. Coordinar la política internacional en materia de ciberseguridad. El Ministerio de Relaciones Exteriores será responsable de esta coordinación con el resto de los ministerios y agencias de gobierno.

2.5. Fomento de la industria y la investigación científica

El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Este fomento se implementará a través de estímulos y fondos dirigidos a la oferta de servicios y productos en ciberseguridad, pero también a través de la generación de una demanda más sofisticada en ciberseguridad, de forma que nuestra industria pueda proteger de mejor forma a las personas y organizaciones, y servir mejor a los intereses del país.

Para avanzar en este objetivo, es necesario:

1. Focalizar la investigación aplicada respecto a aquellos problemas y necesidades en ciberseguridad tanto del sector público como privado. Para ello, se promoverá la creación de institutos de investigación científica aplicada y transferencia tecnológica en la materia, con la finalidad de que potencien la ciberseguridad como un área preferente por parte del sector académico nacional, y que conecten las necesidades de las organizaciones y el sector público con el conocimiento científico existente.

2. Generar incentivos para el emprendimiento tecnológico en ciberseguridad, impulsado por las necesidades de las organizaciones privadas y públicas de nuestro país, particularmente por los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRTs), al alero de grupos de investigación en universidades y centros de investigación. Estos incentivos no se restringirán al ámbito económico, serán amplios y se enfocarán especialmente en las regiones del país distintas de la Región Metropolitana.

3. Revisar los mecanismos de contratación de servicios de ciberseguridad por parte del Estado, para hacerlos más eficientes y expeditos, dando preferencia a la contratación de servicios de ciberseguridad ofrecidos por la industria local.

4. Promocionar los productos y servicios de las empresas locales en ciberseguridad a nivel nacional y en el extranjero, a través de fondos públicos y alianzas público-privadas, y generar incentivos económicos y tributarios para que las empresas existentes puedan ampliar su oferta de servicios en ciberseguridad y ofrecerla de forma preferente al Estado.

5. Fomentar la integración e inclusión de una transversalización de género en el desarrollo del ecosistema de ciberseguridad en nuestro país, generando medidas de acción positiva que permitan aumentar el número de mujeres en roles gerenciales y técnicos en ciberseguridad.

3. Gobernanza del país en ciberseguridad

3.1. Marco normativo

Nuestro país cuenta con un amplio conjunto de normas legales y reglamentarias que se relacionan directa o indirectamente con la ciberseguridad. Dentro de éstas destacan a nivel nacional nuestra propia Constitución Política de la República (artículos 8º, 19, 24, 39 y siguientes) y leyes como la ley Nº 20.285, sobre acceso a la información pública; la ley Nº 19.628, sobre protección de la vida privada; la ley Nº 21.180, sobre transformación digital del Estado; la ley Nº 21.113, que declara el mes de octubre como el mes nacional de la ciberseguridad; 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; la ley Nº 21.521, que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, también denominada "ley FINTECH"; la ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; la ley Nº 19.974, sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia; la ley Nº 18.168, ley general de telecomunicaciones; entre otras.

Adicionalmente, es posible destacar las siguientes normas: decreto supremo Nº 83 del 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; decreto supremo Nº 1.299 del 2004, del Ministerio del Interior y Seguridad Pública, 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; decreto supremo Nº 1 del 2015, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado; decreto supremo Nº 533 del 2015, que crea el Comité Interministerial sobre Ciberseguridad, y su modificación mediante decreto supremo Nº 579 del 2020, ambos del Ministerio del Interior y Seguridad Pública; decreto supremo Nº 273 del 2022, del Ministerio del Interior y Seguridad Pública, que establece obligación de reportar incidentes de ciberseguridad; decreto supremo Nº 14 del 2014, del Ministerio de Economía, Fomento y Turismo, que modifica el decreto supremo Nº 181 del 2002, que aprueba el reglamento de la ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica; decreto supremo Nº 24 del 2019, del Ministerio de Economía, Fomento y Turismo, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada; etc.

A su vez, existen normas sectoriales como la resolución exenta Nº 1381, de 10 de agosto de 2020, de la Subsecretaría de Telecomunicaciones, que aprueba norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones; la resolución exenta Nº 785, de 03 de noviembre de 2021, de la Subsecretaría de Redes Asistenciales que aprueba un Instructivo de seguridad de la información y ciberseguridad para el sector salud; de la Superintendencia de Casinos y Juegos cuya circular Nº119, de abril de 2022, imparte instrucciones relativas a los lineamientos de ciberseguridad

que deben observar las sociedades operadoras y las sociedades concesionarias de casinos de juego; de la Superintendencia de Pensiones que establece un Modelo de Gestión de Seguridad de la Información y Ciberseguridad; la norma de carácter general Nº 454, de fecha 18 de mayo de 2021, de la Comisión para el Mercado Financiero que imparte instrucciones en materia de gestión de Riesgo Operacional y Ciberseguridad, así como de la realización periódica de autoevaluaciones en ambas materias en entidades aseguradoras y reaseguradoras; la directiva Nº32, de fecha 05 de diciembre de 2018, de ChileCompra, que aprueba Recomendaciones para la contratación de servicios en la nube; entre otras.

Por último, a nivel internacional, se puede mencionar el Convenio sobre la Ciberdelincuencia, promulgado a través del decreto supremo Nº 83 del Ministerio de Relaciones Exteriores, de 27 de abril del 2017, y la serie de normas ISO/IEC 27000 que han sido publicadas por el Instituto Nacional de Normalización (INN).

3.2. Institucionalidad actual y futura

La institucionalidad vigente en materia de ciberseguridad se encuentra distribuida en diversos organismos y entidades. Esto hace necesaria la coordinación estratégica de los distintos esfuerzos, de sus roles y funciones, y el establecimiento de prácticas y criterios técnicos comunes, con el objetivo de mejorar la eficiencia y eficacia en el ámbito de la ciberseguridad.

Es de público conocimiento que durante los últimos años nuestro país se ha visto afectado por una serie de incidentes y ataques de ciberseguridad. Esto, sumado a una dispersión normativa e institucional, ha generado la necesidad y urgencia de legislar al respecto. Así, con el reconocimiento de la ciberseguridad como un medio transversal para la protección de las personas, sus derechos, patrimonio y seguridad individual, el gobierno del presidente Gabriel Boric ha impulsado el Proyecto de Ley Marco sobre Ciberseguridad (Boletín Nº 14.847-06), ingresado en el gobierno del presidente Sebastián Piñera.

Dicho proyecto ofrece una respuesta integral a los problemas y desafíos que la ciberseguridad impone, acorde al proceso de transformación digital en que se encuentra inmerso nuestro país, teniendo como ámbito de aplicación a todo el sector público y privado, con obligaciones de ciberseguridad diferenciadas por riesgos y tamaño. Reflejo de aquello es la obligación de determinar los servicios esenciales e identificar a los operadores de importancia vital. En cuanto a la institucionalidad, crea la Agencia Nacional de Ciberseguridad, el Consejo Multisectorial sobre Ciberseguridad, un CSIRT Nacional y el CSIRT de la Defensa Nacional, velando por su coordinación con otros CSIRT Sectoriales que se pudieran originar.

Finalmente, el proyecto de ley propone establecer obligaciones específicas en materia de ciberseguridad para el sector público y el sector privado, incorporando la dimensión de la educación, capacitación, buenas prácticas y ciberhigiene. Además, siguiendo las mejores y más actuales prácticas internacionales, busca fomentar la investigación de vulnerabilidades otorgando protección legal al hacking ético, y promover la notificación de incidentes de ciberseguridad. De aprobarse el proyecto de ley, Chile contará con un marco normativo y una autoridad nacional de ciberseguridad de vanguardia en la región y en el mundo.

Anótese, tómese razón, y publíquese.- GABRIEL BORIC FONT, Presidente de la República.- Carolina Tohá Morales, Ministra del Interior y Seguridad Pública.- Albert van Klaveren Stork, Ministro de Relaciones Exteriores.- Mario Marcel Cullell, Ministro de Hacienda.- Álvaro Elizalde Soto, Ministro Secretario General de la Presidencia.- Nicolás Grau Veloso, Ministro de Economía, Fomento y Turismo.- Marco Antonio Ávila Lavanal, Ministro de Educación.- Luis Cordero Vega, Ministro de Justicia y Derechos Humanos.- Juan Carlos Muñoz Abogabir, Ministro de Transportes y Telecomunicaciones.- Aisén Etcheverry Escudero, Ministra de Ciencia, Tecnología, Conocimiento e Innovación.

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

LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

P r o y e c t o d e l e y:

PROTECCION DE DATOS DE CARACTER PERSONAL

Título Preliminar

Disposiciones generales

Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

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. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

Artículo 2°.- Para los efectos de esta ley se entenderá por:

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

d) Dato caduco, el 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 norma expresa, por el cambio de los hechos o circunstancias que consigna.

e) Dato estadístico, el 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, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

m) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera 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.

n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Artículo 3°.- En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas.

El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

Título I

De la utilización de datos personales

Artículo 4°.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Artículo 5º.- 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.

Frente a un requerimiento de datos personales 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, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

Artículo 6°.- Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.

Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

Artículo 7°.- 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 campo.

Artículo 8°.- En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales.

El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

Artículo 9°.- Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Prohíbese la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda.

Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Título II

De los derechos de los titulares de datos

Artículo 12.- Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, 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.

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

Si los datos personales cancelados 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 les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

Artículo 13.- El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

Artículo 14.- Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.

Artículo 15.- No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras 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.

Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva.

Artículo 16.- Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente.

El procedimiento se sujetará a las reglas siguientes:

a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes.

h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales, o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a lo dispuesto en los artículos 17 y 18.

La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

Título III

De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial

Artículo 17.- Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. Se exceptúa la información relacionada con los créditos concedidos por el

Instituto Nacional de Desarrollo Agropecuario a sus usuarios, y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentren con alguna modalidad pendiente.

También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas; tampoco las deudas contraídas con instituciones de educación superior de conformidad a las leyes números 18.591 y 19.287, ni aquellas adquiridas con bancos o instituciones financieras de conformidad a la ley Nº 20.027, o en el marco de las líneas de financiamiento a estudiantes para cursar estudios en educación superior, administradas por la Corporación de Fomento de la Producción, ni alguna deuda contraída con la finalidad de recibir para sí o para terceros un servicio educacional formal en cualquiera de sus niveles; ni las deudas contraídas con prestadores de salud públicos o privados y empresas relacionadas, sean instituciones financieras, casas comerciales u otras similares, en el marco de una atención o acción de salud ambulatoria, hospitalaria o de emergencia sean éstas consultas, procedimientos, exámenes, programas, cirugías u operaciones; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura.

Las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el período de cesantía que afecte al deudor.

Para estos efectos, la Administradora de Fondos de Cesantía comunicará los datos de sus beneficiarios al Boletín de Informaciones Comerciales sólo mientras subsistan sus beneficios para los efectos de que éste bloquee la información concerniente a tales personas.

Sin embargo, las personas que no estén incorporadas al seguro de cesantía deberán acreditar dicha condición ante el Boletín de Informaciones Comerciales, acompañando el finiquito extendido en forma legal o, si existiese controversia, con el acta de comparecencia ante la Inspección del Trabajo, para los efectos de impetrar este derecho por tres meses renovable hasta por una vez. Para que opere dicha renovación se deberá adjuntar una declaración jurada del deudor en la que manifieste que mantiene su condición de cesante.

El bloqueo de datos será sin costo para el deudor.

No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral.

Las entidades responsables de la administración de bancos de datos personales no podrán señalar bajo ninguna circunstancia, signo o caracterización que la persona se encuentra beneficiada por esta ley.

NOTA: Los artículos 1º, 2º y 3º transitorios de la LEY 19812, publicada el 13.06.2002, establecen en relación con el presente artículo, lo siguiente: "Artículo 1° transitorio.- Los responsables de los registros o bancos de datos personales que traten información señalada en el artículo 17 de la ley N° 19.628 no podrán comunicarla cuando se refiera a obligaciones que, a la fecha de publicación de esta ley, hayan sido pagadas o se hayan extinguido por otro modo legal. Asimismo, no podrán comunicar los datos relativos a esas obligaciones que se hayan hecho exigibles antes del 1º de mayo de 2002 y se encuentren impagas, siempre que el total de obligaciones impagas del titular que comunique el registro o banco de datos a la fecha de publicación de esta ley sea inferior a $2.000.000 por concepto de capital, excluyendo intereses, reajustes y cualquier otro rubro. En el caso de los incisos anteriores, tampoco podrá proporcionarse información al titular de los datos, ni comunicarse el hecho de que éste haya sido beneficiado con esas disposiciones. Artículo 2º transitorio.- Los responsables de los registros o bancos de datos personales que comuniquen información sobre las obligaciones a que se refiere el artículo 17 de la ley Nº 19.628 eliminarán todos los datos relacionados con créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios. Artículo 3º transitorio.- Los deudores del Banco del Estado de Chile que al 30 de septiembre de 1999 obtuvieron créditos en el marco del programa de créditos para establecimiento por cuenta propia de chilenos retornados y que hayan optado, dentro del plazo establecido, a los beneficios que les otorga la ley Nº 19.740, una vez aclarada la morosidad y previa solicitud, serán borrados definitivamente del o los registros históricos que existan sobre los documentos señalados en el artículo 17.".

Artículo 18.- En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal.

Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes.

Artículo 19.- El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente.

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres

días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16.

Título IV

Del tratamiento de datos por los organismos públicos

Artículo 20.- El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.

Artículo 21.- Los organismos públicos que sometan a tratamiento 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 la pena.

Exceptúase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11 y 18.

Artículo 22.- El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

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.

Título V

De la responsabilidad por las infracciones a esta ley

Artículo 23.- La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

Título Final

Artículo 24.- Agrégase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario:

''Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.''.

Disposiciones transitorias

Artículo 1°.- Las disposiciones de esta ley, con excepción del artículo 22, entrarán en vigencia dentro del plazo de sesenta días, contados desde la fecha de su publicación en el Diario Oficial.

Los actuales registros o bancos de datos personales de organismos públicos se ajustarán a las disposiciones de este cuerpo legal, a contar de su entrada en vigencia.

Lo dispuesto en el artículo 22 comenzará a regir un año después de la publicación de esta ley. Sin perjuicio de lo anterior, los organismos públicos que tuvieren a su cargo bancos de datos personales deberán remitir los antecedentes a que se refiere dicho precepto con anterioridad, dentro del plazo que fije el reglamento.

Artículo 2°.- Los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la presente ley tendrán los derechos que ésta les confiere.

Artículo 3°.- Las normas que regulan el Boletín de Informaciones Comerciales creado por el decreto supremo de Hacienda N° 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley.''.

Habiéndose cumplido con lo establecido en el N° 1º del artículo 82 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 18 de agosto de 1999.- EDUARDO FREI RUIZ-TAGLE, Presidente de la República.- José Miguel Insulza Salinas, Ministro Secretario General de la Presidencia.- María Soledad Alvear Valenzuela, Ministra de Justicia.- Germán Quintana Peña, Ministro de Planificación y Cooperación.

Lo que transcribo a Ud., para su conocimiento.- Saluda Atte. a Ud., Carlos Carmona Santander, Subsecretario General de la Presidencia de la República.

DECRETO 273 ESTABLECE OBLIGACIÓN DE REPORTAR INCIDENTES DE CIBERSEGURIDAD

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA; SUBSECRETARÍA DEL INTERIOR

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.