

El Presidente firmó ayer la normativa que ingresará al Congreso:

# Gobierno presenta proyecto de ley de delitos informáticos con penas de hasta 5 años

La legislación tipifica siete delitos en donde incluye el acceso ilícito a sistemas o "hackeo". Además, sumó técnicas especiales de investigación como agentes encubiertos.



CEREMONIA.— En la firma del proyecto en La Moneda, el Presidente Piñera estuvo acompañado por los ministros de Interior y Justicia, Andrés Chadwick y Hernán Larraín, respectivamente, y el asesor presidencial de Ciberseguridad, Jorge Atton.

“Una cosa muy importante es estar consciente de estos ataques, porque son una alerta, una luz amarilla o roja para saber dónde están nuestros puntos más débiles”.

SEBASTIÁN PIÑERA  
PRESIDENTE DE LA REPÚBLICA

“Tenemos una brecha y es-tamos quedando muy atrasados respecto al resto de los países”.

JORGE ATTON  
ASESOR PRESIDENCIAL DE  
CIBERSEGURIDAD

## Expertos anticipan mayor seguridad para las empresas

**“ESTO ES UN GRAN AVANCE PARA EL PAÍS, PARA LAS PERSONAS Y OBTIVAMENTE PARA LAS EMPRESAS”**

Marcelo Zanotti  
Socio líder de Consultoría en Riesgo de EY Chile

Para el socio líder de Consultoría en Riesgo de EY Chile, Marcelo Zanotti, la situación del país en materia de legislación de delitos no era buena, por lo que asegura que “es un gran avance para el país, las personas y, obviamente, las empresas”. Zanotti explicó también que por el hecho de que la legislación ahora vaya a considerar un catálogo más amplio de delitos informáticos, se tendería a pensar que los estándares de seguridad de las empresas. “Esto es una tarea que debe ser realizada al interior de cada compañía, considerando los riesgos y vulnerabilidades actuales que estas tengan”, advirtió.

### EN LOS NEGOCIOS ONLINE

Ignacio Concha  
Socio de Deloitte Legal

Ignacio Concha, socio de Deloitte, señaló que si bien no se conoce el detalle del proyecto, este permitiría a las empresas perseguir a quienes atacan sus sistemas. Con ello, dijo, “la ley otorgará mayor seguridad en los negocios online”. Por otro lado, sostuvo que será necesario que las empresas establezcan mecanismos de control conforme a la nueva legislación, para así evitar que alguien de la organización incurra en las conductas sancionadas. “Los directores deberán velar por establecer las políticas relevantes en sus empresas para no ser considerados negligentes en el tema”, dice. Concha añade que hay aspectos que son esperados, como la ampliación y actualización de los tipos penales. No obstante, destaca otros que son “novedosos”, como el establecimiento de técnicas especiales de investigación en casos específicos.

## Principales materias del Instructivo de Ciberseguridad

El Instructivo de Ciberseguridad que firmó ayer el Presidente Piñera fija obligaciones a los distintos servicios públicos del Estado y una Gobernanza Transitoria de Ciberseguridad.

Esta última, que será dependiente del Ministerio del Interior, armará el organigrama para definir finalmente cómo se va a transitar a un nuevo proyecto de ley que van a presentar a mediados del próximo año.

Algunas de las principales materias que cubre el instructivo son la designación de un encargado de ciberseguridad de alto nivel en cada servicio, que será responsable de implementar normas y estándares que garanticen la seguridad informática en su repartición; la aplicación y actualización de la normativa técnica sobre ciberseguridad; medidas internas de ciberseguridad; servicios que tienen infraestructuras críticas de la información; vigilancia y análisis del funcionamiento de infraestructura crítica para los sistemas de información de las diferentes instituciones públicas; reporte obligatorio de incidentes de ciberseguridad y respuesta a incidentes de ciberseguridad por los órganos de la Administración del Estado.

En base a esta experiencia se presentará en los próximos meses el proyecto de ley Marco de Ciberseguridad, que establecerá la Gobernanza Definitiva que establece la política nacional de Ciberseguridad.

El diputado Jorge Alessandri (UDI) valoró el anuncio del Presidente en materia de ciberseguridad y dijo que evalúa muy positivamente que el Estado tenga un ordenamiento particular para cuidarse de los ataques.

definir la gobernanza definitiva que se va a implementar en el país, es decir, una institucionalidad a cargo del tema, tanto para el sector público como para el privado.

Mientras tanto, el instructivo establece las obligaciones para los distintos servicios del Estado y una gobernanza transitoria —que estará en el Ministerio del Interior— que será responsable de implementar las diferentes políticas y normas; crear los centros de coordinación ante incidencias informáticas en los sectores, tanto públicos como privados.

El instructivo señala que cada servicio deberá tener un encargado del tema. “Cada organismo o servicio público tiene que designar una persona que esté a cargo y se haga responsable de la ciberseguridad de ese organismo”, dijo el Presidente en su discurso (ver relacionado).

El Ejecutivo también le pondrá suma urgencia al proyecto de ley de datos personales que se encuentra en el Congreso.

## Los delitos que se tipifican y sus sanciones

### 1 Perturbación informática

Sanciona a quienes maliciosamente obstaculicen o perturben el funcionamiento de un sistema informático a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos. La pena que considera esta infracción es de presidio menor en su grado máximo (541 días a cinco años).

Si además se hiciera imposible la recuperación del sistema informático, se aplicará la pena de presidio menor en su grado máximo (3 años y 1 día a 5 años). Por ejemplo, alteración de sistemas informáticos que hacen funcionar los sistemas de transporte, financieros o telecomunicaciones, entre otros.

### 2 Acceso ilícito

Se considerará un delito el acceso ilícito o *hackeo* a todo o a una parte del sistema informático. El culpable arriesga una pena de presidio menor en su grado mínimo o una multa de 11 a 20 UTM.

### 3 Intercepción o interferencia

En caso de intercepción o interferencia indebida y maliciosa de las transmisiones no públicas entre sistemas informáticos, se arriesga una pena de presidio menor en su grado mínimo.

### 4 Daño informático

Cuando se alteren, borren o destruyan datos informáticos, causando daños serios al titular de los mismos, se arriesga una pena de presidio menor en su grado medio.

### 5 Delitos de falsificación informática

Comprende la introducción maliciosa, alteración, borrado, deterioro, daño, destrucción o supresión que genere datos no auténticos con el propósito de que sean tomados o utilizados como “auténticos”. Esto será sancionado con las penas de presidio menor en cualquiera de sus grados, previstas en el Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público.

### 6 Fraude informático

El delito de fraude informático será para sancionar a quien defraude a otro y con la finalidad de obtener un beneficio económico ilícito para sí o un tercero, utilizando la información contenida en un sistema informático o aprovechándose de la alteración, daño o supresión de documentos electrónicos. Las sanciones van a depender del perjuicio.

### 7 Abuso de dispositivos

Para quienes usen dispositivos que alteren la integridad de datos informáticos, perturben el sistema informático, permitan el acceso ilícito e interceptación ilícita, o aquellos contenidos en el artículo 5º de la Ley sobre Extravío, Robo o Hurto de Tarjetas de Crédito o Débito. La pena será de presidio menor en su grado mínimo (61 días a 540 días) y multa de 5 a 10 UTM. Por ejemplo, mecanismos para clonar tarjetas de crédito, copiar bandas magnéticas o de sistemas de acceso restringido, los llamados *skimmings*.

El ingreso de este proyecto es parte de la Política Nacional de Ciberseguridad que prepara el Gobierno para enfrentar los riesgos que puede traer del mundo digital.

Además de ingresar las modificaciones a normativa de delitos informáticos el Presidente firmó ayer un Instructivo Presidencial de Ciberseguridad.

Sin embargo, a mediados del próximo año se pretende presentar un nuevo proyecto de Ley Marco de Ciberseguridad que va

MARÍA JESÚS COLOMA

Tras los múltiples ciberataques que han ocurrido durante el año, como el *hackeo* y robo al Banco de Chile y las filtraciones de datos de tarjetas de créditos, el Gobierno dio a conocer una nueva medida para enfrentar los riesgos del mundo digital.

El Presidente presentó y firmó ayer un nuevo proyecto de ley que modifica la actual legislación de delitos informáticos (Ley 19.223) que fue promulgada en 1993.

“La normativa se encuentra absolutamente superada por el progreso de la tecnología; esa ley respondía a un Chile que recién se asomaba al mundo del Internet”, dijo el mandatario.

En la misma línea, agregó: “Y un dato relevante es el que nos entrega la Policía de Investigaciones, que los delitos informáticos aumentaron el 2017 en un 74% respecto al año anterior. Ese es su crecimiento exponencial, al cual tenemos que literalmente ponerle atajo y ponerle freno”.

El proyecto propone tipificar nuevos delitos informáticos, los que llegan a siete. Por estos, los culpables arriesgan penas de hasta cinco años y multas de hasta 30 UTM, es decir, unos \$14 millones (ver recuadro).

Asimismo, la normativa contiene mejoras procesales en las que destaca la legitimación del Ministerio del Interior y Seguridad de presentar querrelas en caso de interrupción a servicios de utilidad pública por delitos informáticos; fija técnicas especiales de investigación en casos específicos, que podrían ser a través de agentes encubiertos, informantes, entrega vigilada de información e interceptación de documentos. Además establece procedimientos dictados por el Fiscal Nacional sobre manipulación de evidencia electrónica.

Por último, el proyecto establece definiciones sobre el sistema y los datos informáticos de acuerdo al Convenio de Budapest (estándar que se usa en la Unión Europea).

“En esta preocupación y compromiso de que la revolución tecnológica y el mundo digital estén al servicio y no se transformen en enemigos de los ciudadanos, el Gobierno está adecuando esta ley incorporando nuevas figuras penales”, comentó el jefe de Estado.

El proyecto que ingresará al Congreso fue valorado por el asesor presidencial de ciberseguridad, Jorge Atton. “Esto es parte del compromiso del Presidente de acelerar y transformar la política nacional de ciberseguridad en una estrategia de implementación de todas las tareas que requiere Chile”, afirmó.

### Política Nacional de Ciberseguridad

El ingreso de este proyecto es parte de la Política Nacional de Ciberseguridad que prepara el Gobierno para enfrentar los riesgos que puede traer del mundo digital.

Además de ingresar las modificaciones a normativa de delitos informáticos el Presidente firmó ayer un Instructivo Presidencial de Ciberseguridad.

Sin embargo, a mediados del próximo año se pretende presentar un nuevo proyecto de Ley Marco de Ciberseguridad que va

ANDRÉS FÉREZ GUERRA