

71% DE LAS EMPRESAS QUE VENDEN O DISTRIBUYEN APARATOS RELACIONADOS CON INTERNET DE LAS COSAS NO SE HACE CARGO DE FUGA DE DATOS

- **El SERNAC realizó un estudio que revisó el mercado del Internet de las Cosas en Chile y encuestó a las empresas que venden o distribuyen dispositivos relacionados.**
- **El análisis concluye que existen vacíos que podrían afectar a los consumidores en materia de protección de sus derechos y asimetría de información.**

El SERNAC realizó un estudio para visualizar riesgos y la necesidad de protección en relación al uso de dispositivos basados en "Internet de las Cosas".

A nivel básico, se entiende la internet de las cosas (*IoT* -por sus siglas en inglés) como dispositivos que, gracias a su capacidad computacional, pueden estar conectados a internet y con ello comunicarse con otros dispositivos, enlazando así el mundo físico con el mundo digital.

Por ejemplo, existen dispositivos que permiten comandar tareas como encender las luces y televisión, decir el estado del tiempo, u otras más elaboradas como controlar la lavadora, el refrigerador o cerraduras de puertas. También existen dispositivos de uso doméstico que se adaptan para interactuar con otros, por ejemplo, con el celular, como automóviles, relojes, aspiradoras robot, relojes inteligentes, cámaras de seguridad, etc.

Las conexiones de dispositivos de internet de las cosas a la red han crecido exponencialmente, estimándose que el número de conexiones para el año 2030 bordearía los 28 mil millones.

Para el Director del SERNAC, Lucas Del Villar, es importante revisar los riesgos y desafíos de estas tecnologías para proteger los derechos de los consumidores, por ejemplo, en materia de protección de datos y entrega de información sobre sus riesgos.

Indica que una de las complejidades de estos sistemas es que involucran productos y servicios al mismo tiempo, pues se necesita un aparato y un proveedor de software e Internet, pero además, existen distintos actores involucrados por lo que es difícil para el consumidor identificar responsabilidades a la hora de problemas.

Asimismo, existen riesgos asociados a la "obsolescencia programada" o el hecho de que el aparato deje de servir cuando se requiere una actualización. También se evidencian desafíos asociados a la ciberseguridad y protección de datos personales.

La autoridad explica que, según diferentes preocupaciones expresadas por la misma OCDE, la falta de actualización del software no debe implicar de modo arbitrario, el fin del funcionamiento del dispositivo.

En la misma línea, el año 2017 Consumers International hizo recomendaciones a la regulación de la venta de este tipo de dispositivos teniendo en cuenta los potenciales riesgos frente a los cuales los consumidores podrían verse enfrentados a la hora de comprar y utilizar estos dispositivos.

Existen experiencias en países como Singapur o Reino Unido acerca del etiquetado de los productos, señalando qué tipo de datos son utilizados por el dispositivo o el nivel de seguridad que ofrece este frente a vulnerabilidades o ataques informáticos.

HALLAZGOS

El SERNAC aplicó una encuesta a 74 empresas distribuidoras o vendedoras de aparatos relacionados con Internet de las Cosas (con una tasa de respuesta del del 47%), y se realizaron entrevistas nacionales e internacionales pautadas a diversos especialistas en las áreas involucradas.

En lo relacionado a la **transferencia de datos a terceros**, ya sea por fugas de información o por prácticas empresariales, el **71% indica no hacerse responsable por vulnerabilidades frente a la fuga de datos**, lo cual implica un desentendimiento respecto a la ciberseguridad de los dispositivos.

En lo relacionado a **políticas de protección de datos** y alcance, **40%** de las empresas encuestadas señalan que ninguno o sólo algunos de sus dispositivos están afectos a políticas de seguridad de información y privacidad de los datos. Un 43% afirma que sí cuenta con esas políticas para todos los dispositivos comercializados.

En general, las empresas señalan que cuentan con mecanismos de apoyo hacia el consumidor en caso de problemas con el software. No obstante, en un 11% de los casos, las empresas indican que son los fabricantes de los dispositivos o de los software quienes deben hacerse cargo de esta situación o que no existe un servicio técnico ofrecido por las empresas proveedoras.

Respecto a la propiedad del software, el **64%** de las empresas señalan que la propiedad no recae sobre el consumidor, sino sobre el fabricante del software (37%) o la empresa fabricante del dispositivo (27%). En este sentido, las condiciones de su utilización podrían quedar condicionadas al fabricante, más allá de la compra del dispositivo por parte del consumidor.

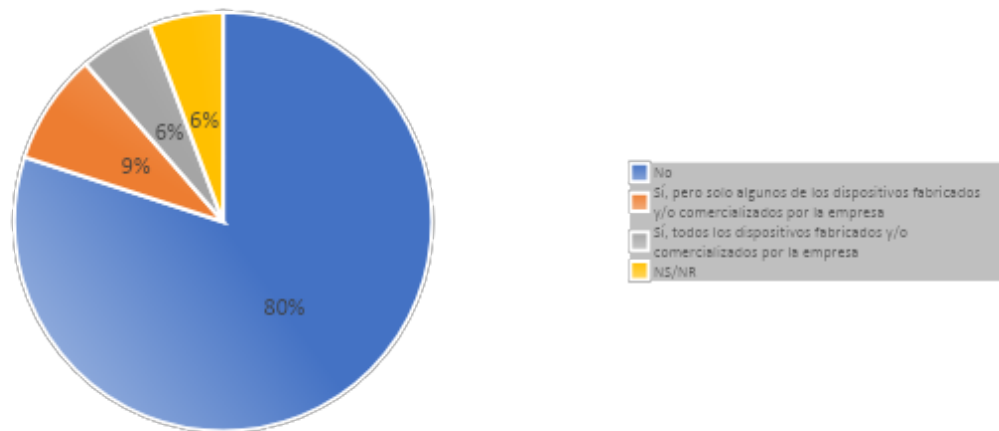
A las empresas también se les consultó respecto de las políticas que limiten los años de vida útil de los dispositivos, donde el 14% admite estar regidas por políticas que limitan la duración de los dispositivos (6% de las empresas encuestadas aplica para todos sus productos, mientras que para el 8% solo

aplica para algunos de los dispositivos). El 80% señala no encontrarse afectos a este tipo de lineamientos.

Respecto a las razones por las cuales se realiza dicha consideración, las empresas señalan en un 67% de los casos que dicha política se debe al "diseño del dispositivo que provoca el fin de la vida útil tras un determinado número de utilidades u otro factor temporal" , mientras que el 33% señala que se debe a razones de actualización y soporte del dispositivo, una de las posibilidades consideradas por la Unión Europea respecto a la razonabilidad de la duración del soporte y actualización que puede dar una empresa a un dispositivo.

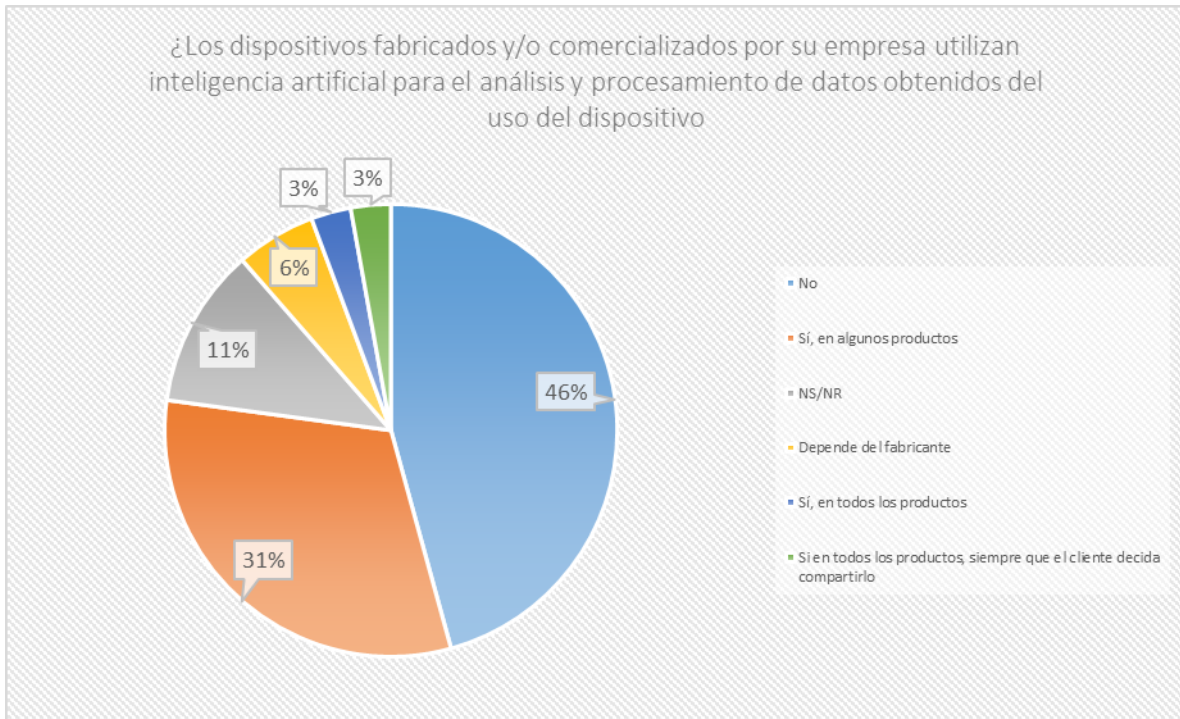
N

¿Los dispositivos que fabrica y/o comercializa están regidos por una política que limite los años de vida útil del dispositivo?



Respecto a **temas de ciberseguridad**, sólo dos de las empresas consultadas señalan elementos de certificación en este aspecto, como lo es la certificación ISO 27001 sobre sistemas de seguridad de la información o elementos de encriptación. Por tanto, en general, es posible deducir que los aspectos de ciberseguridad no forman parte de la consideración que se tiene respecto a la seguridad y calidad de este tipo de dispositivos.

Referente al **uso de inteligencia artificial**, el 37% de las empresas señala que sus productos hacen uso de esta técnica de procesamiento de datos, mientras que el 46% señala que no. No obstante, existen respuestas que señalan que **se desconoce si el fabricante utiliza o no estos algoritmos**, o que su uso queda a discreción del fabricante, evidenciando una falta de conocimiento respecto a la cadena de valor de sus productos.



En lo relativo a **qué tipo de datos son utilizados por las empresas**, en el 16% de los casos señalan que los datos recolectados son solo los datos de uso del dispositivo, seguido de 14% que señalan utilizar datos de informes de errores de dispositivos. 10% de las empresas encuestadas indican utilizar datos que permiten perfilar a los usuarios, mientras que en un 8% de los casos las empresas indican consumir datos personales de los consumidores y un 4% datos sensibles como gustos, geolocalización entre otros. No obstante, llaman la atención respuestas como que la empresa no captura datos de los consumidores debido a que **queda a discrecionalidad de los fabricantes de los dispositivos o que desconocen este tipo de situación**.

Respecto a la **información entregada previa a la venta del dispositivo**, no todas incluyen información relevante acerca del funcionamiento, políticas, términos y condiciones de los dispositivos de internet de las cosas que se venden a los consumidores.

El Director del SERNAC subraya que estos resultados confirman la necesidad de seguir profundizando el análisis y vigilancia pues se evidencian asimetrías de información, vulnerabilidad de los datos de las personas y un concepto del derecho de propiedad difuso.

Indica que los consumidores deben estar informados acerca del consumo de los datos que las empresas hacen uso, como también la cadena de valor del dispositivo debe estar correctamente identificada para poder sopesar las

responsabilidades que tienen los distintos actores en caso de falla de sus dispositivos.