TALSOFT
SECURITY

TENDENCIAS 2017
CIBERSEGURIDAD

consultas@talsoft.com.ar

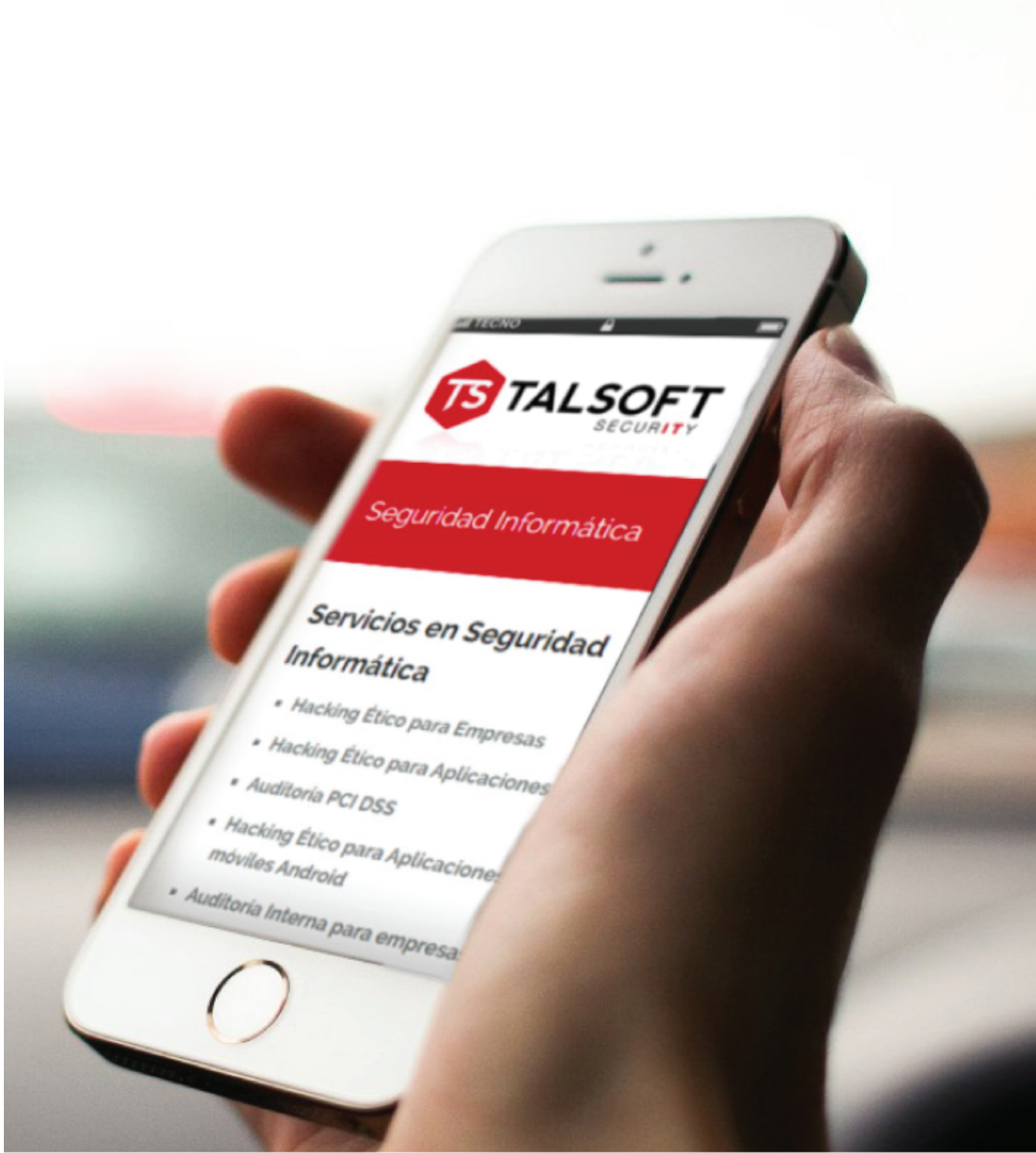
www.talsoft.com.ar

Tendencias 2017

La privacidad y seguridad informática es uno de los mayores problemas para las empresas y, cada vez más, para los usuarios que sienten la preocupación de dejar la puerta abierta a sus datos personales para fines comerciales ilícitos.

La nueva era denominada "Internet de las Cosas", se ha demostrado que no hay ningún aparato electrónico conectado a internet que sea 100% seguro. Los ciberdelincuentes lo saben y adaptan sus técnicas a los nuevos vectores de ataques.

El uso de dispositivos móviles, ataques a infraesctruturas críticas o la hiperconectividad son algunas de las predicciones clave sobre ciberseguridad que se mantendrán para 2017, según los pronósticos de la firma de seguridad informática Check Point.

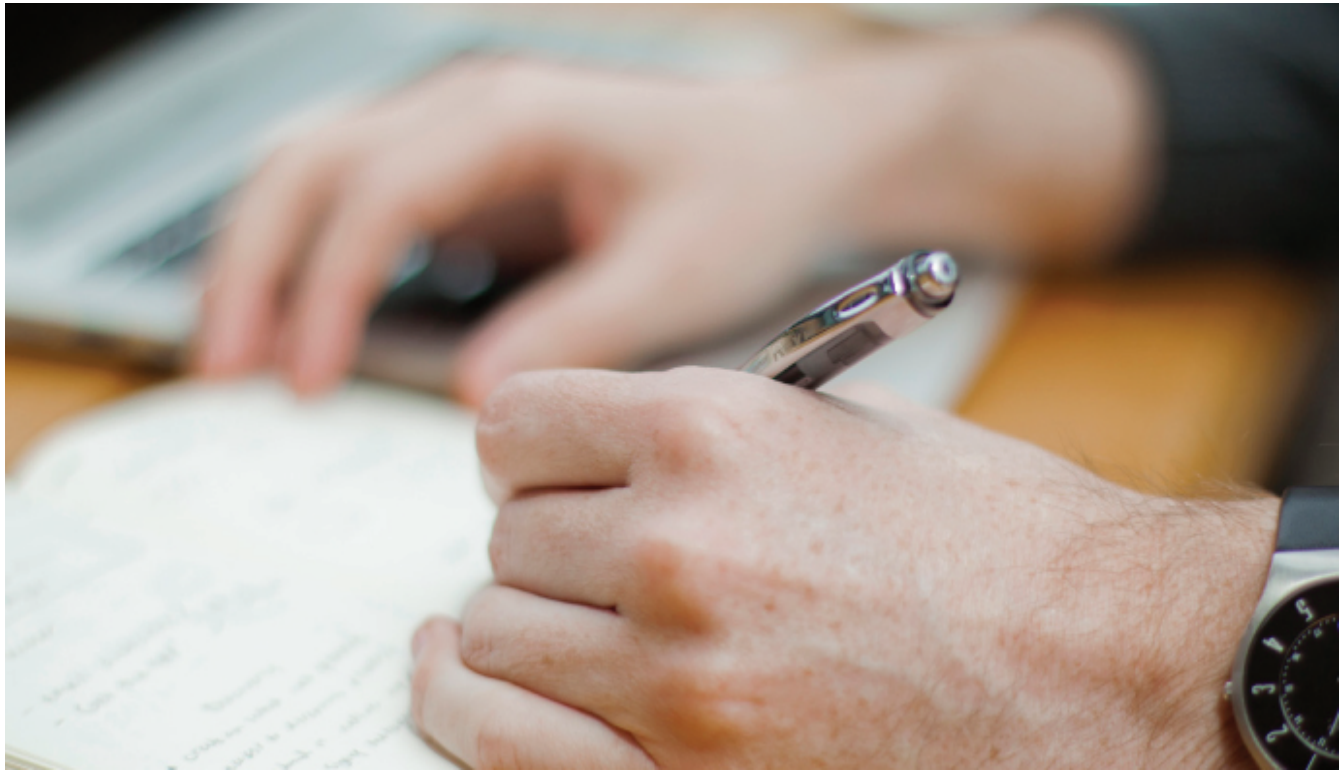


Ataques a dispositivos móviles

Los dispositivos móviles son el punto de mira de los ciberdelincuentes. Desde hace algún tiempo es un mito que este tipo de aparatos están libres de virus informáticos y no son objeto de ataques.

Nada más lejos de la realidad. En los últimos años el uso de «smartphones» ha aumentado un 394% y el de tabletas un 1.700%.

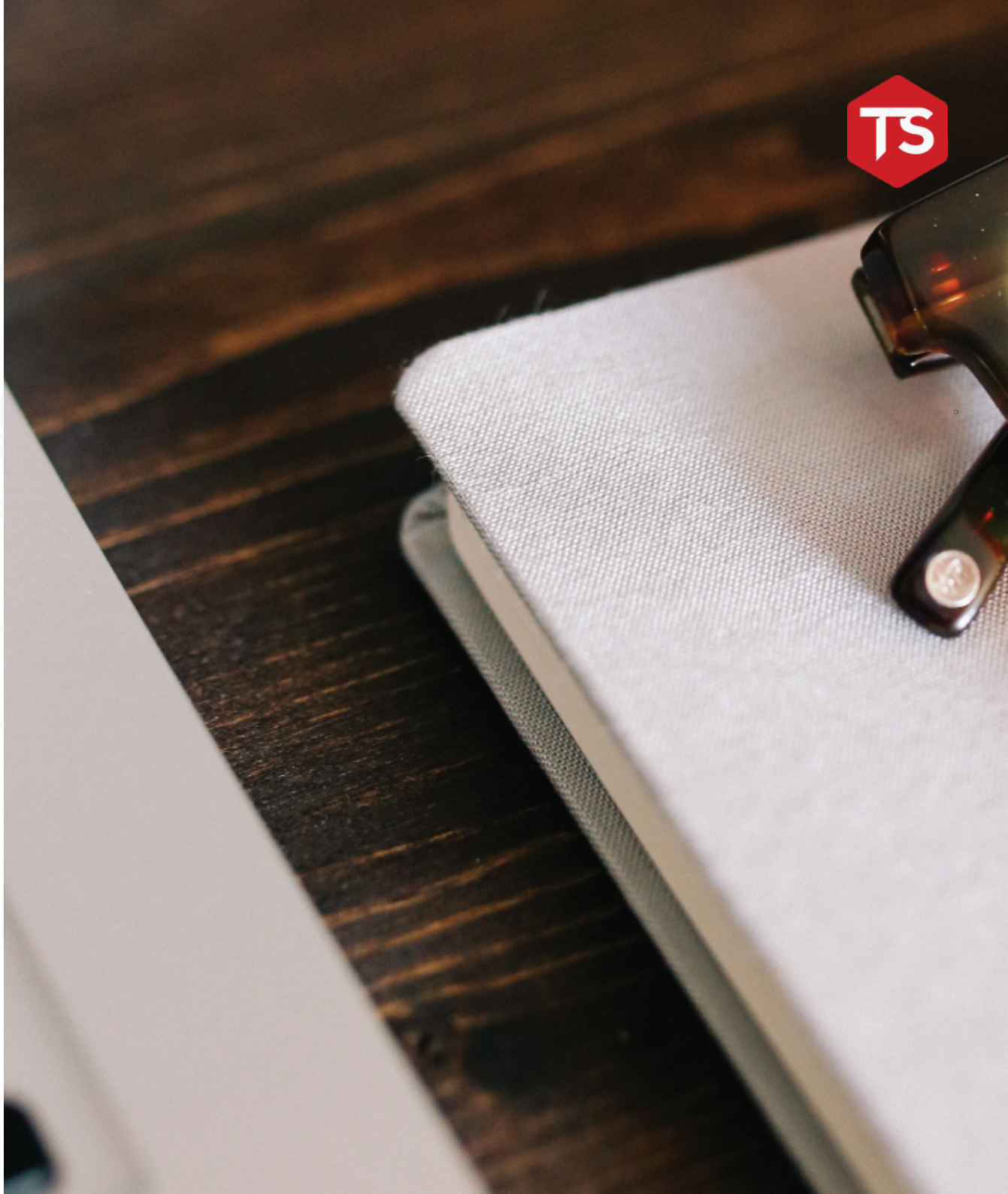
A la luz de estos datos, no es de extrañar que los ataques a terminales móviles sigan creciendo. Uno de cada cinco empleados será en 2017 el responsable de alguna brecha de seguridad que afecte a datos corporativos.
Lo harán, involuntariamente, a través de malware móvil o de redes WiFi maliciosas.



El “Internet de las Cosas” (IOT)

Los expertos lo tienen claro: actualizar y parchear dispositivos inteligentes puede suponer un riesgo, especialmente
si sus desarrolladores no han tenido en cuenta la seguridad como ha sucedido recientemente en el mayor ciberataque de la última década.

«En el 2017 las compañías deben estar preparadas para luchar contra ciberataques dirigidos a todo tipo de elementos conectados,
como por ejemplo las impresoras»,
aseguran.



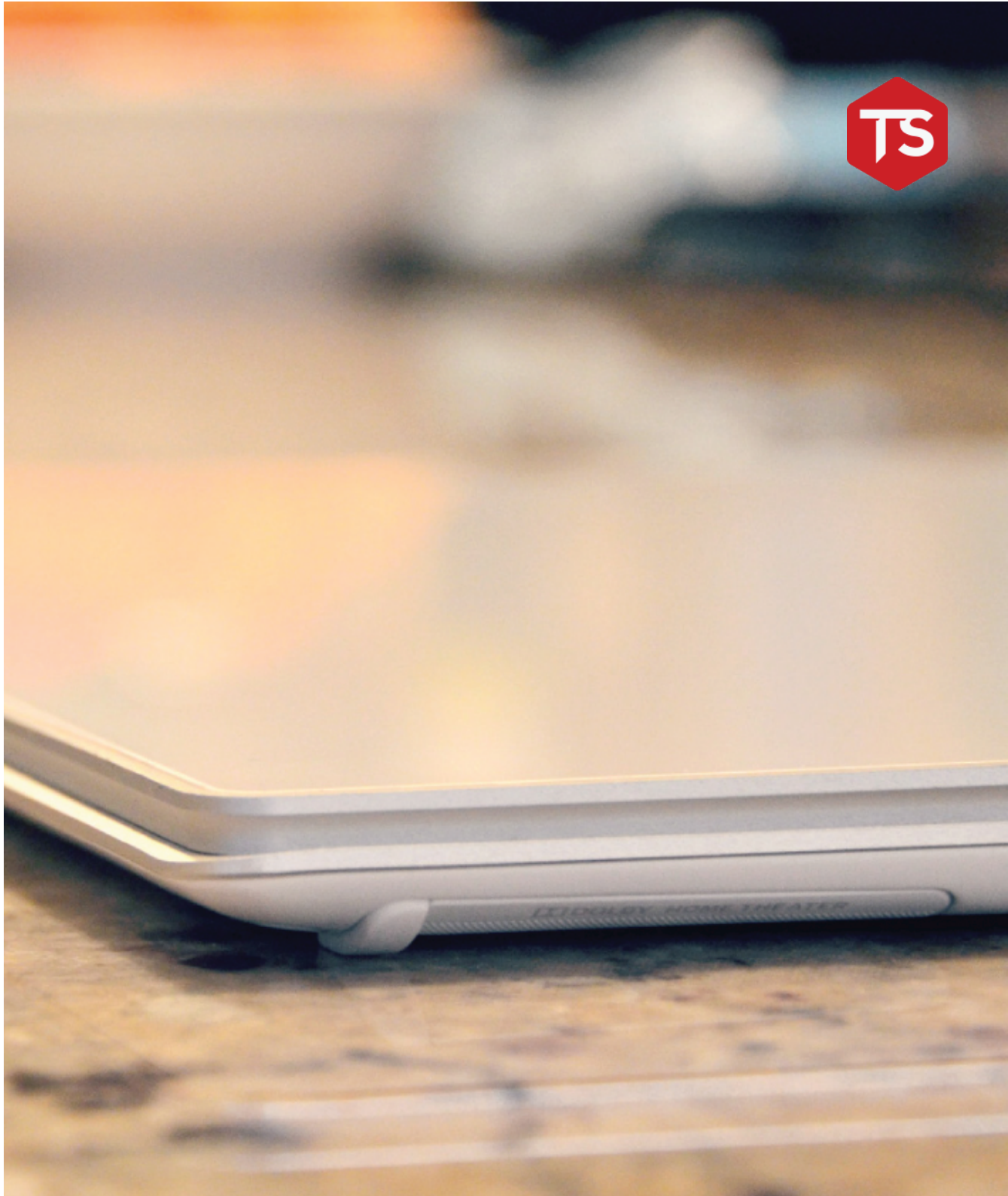
Dispositivos Industriales

Se espera que en 2017 se produzcan nuevas ofensivas contra el «Internet de
las Cosas» de perfil industrial.

La convergencia entre las tecnologías de la información y la operativa las hace más vulnerables.

"Las empresas tendrán que extender los controles de seguridad de ambos sistemas. Además, deberán implementar soluciones de prevención de amenazas para ambos ecosistemas".

Y es que de acuerdo con la investigación realizada por Fortinet, el 50% de los responsables de tecnología consideran que la mejor respuesta al incremento de brechas de seguridad.

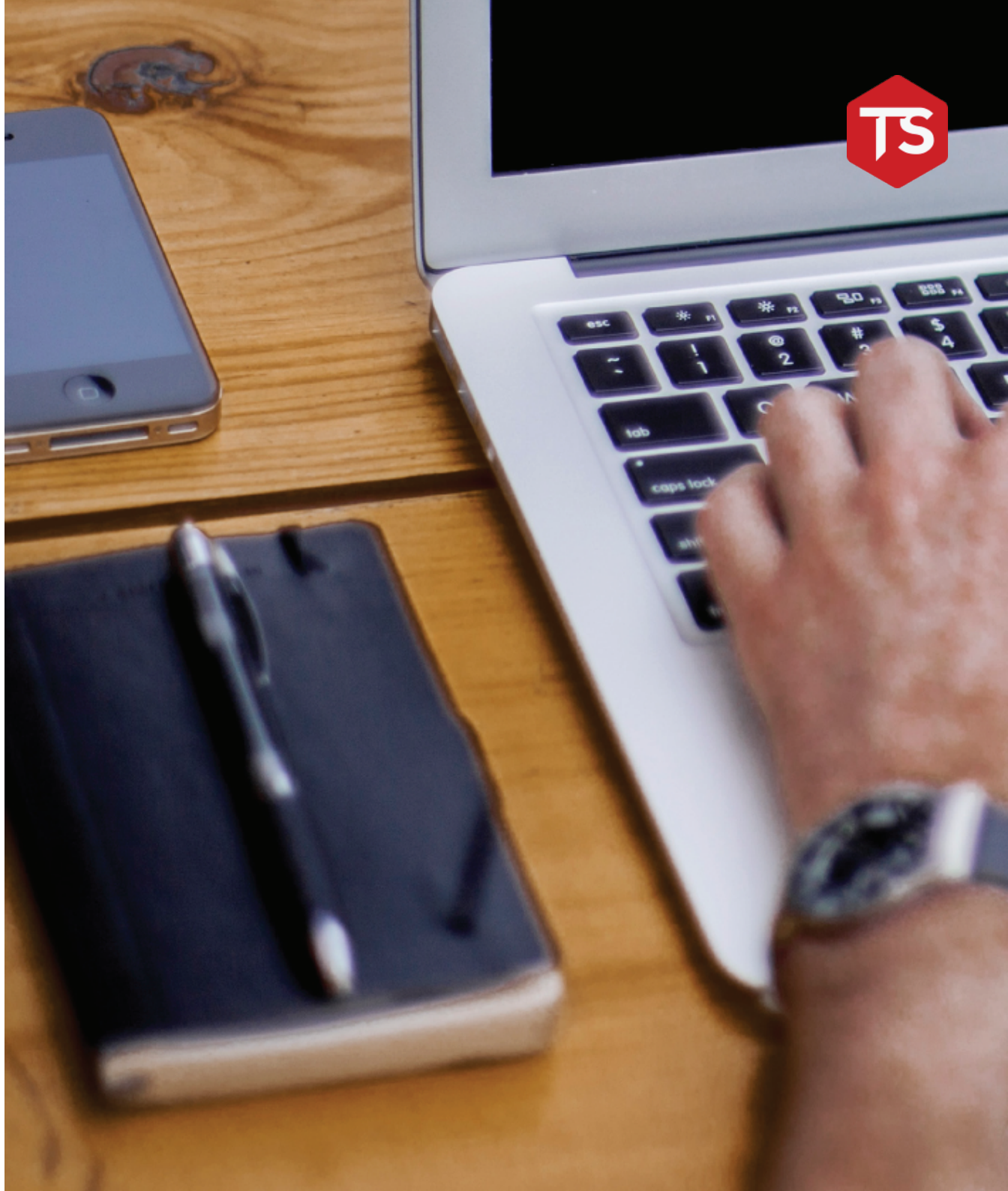


Infraestructuras críticas

Como ha quedado demostrado en los últimos años, los ciberdelincuentes han fijado sus intereses en demostrar las vulnerabilidades de las llamadas "infraestructuras críticas", consideradas como estratégicas, y que, en caso de ser atacadas, pueden poner en riesgo la seguridad nacional o la economía.

A comienzos de 2016, de hecho, se desveló el primer apagón causado por ciberdelincuentes.

Según los expertos, "los responsables de seguridad deben prepararse para posibles ataques a sus redes y sistemas,
provenientes de tres actores potenciales: países, terrorismo y criminales organizados".



Aumento de “Secuestros online” y Amenazas

Han crecido los ataques de “ransomware” -secuestro virtual- que afectan a centros de datos basados en la nube.
“Cuantas más empresas se pasen al cloud, más ataques de este tipo se dirigirán a sus infraestructuras emergentes.
Lo harán tanto a través de archivos encriptados que se propaguen de cloud a cloud como con hackers que utilicen la nube como un multiplicador de volumen”.
Otro vector de ataque que últimamente está creciendo son los “Amenazas cibernéticas” que atentan contra los individuos y empresas víctimas de amenazas a sus familias o socios, con diferentes objetivos con el fin desde presionar o realizar un acto delictivo.

Fuente: abc.es

TALSOFT
SECURITY

¡MUCHAS GRACIAS!

consultas@talsoft.com.ar

www.talsoft.com.ar