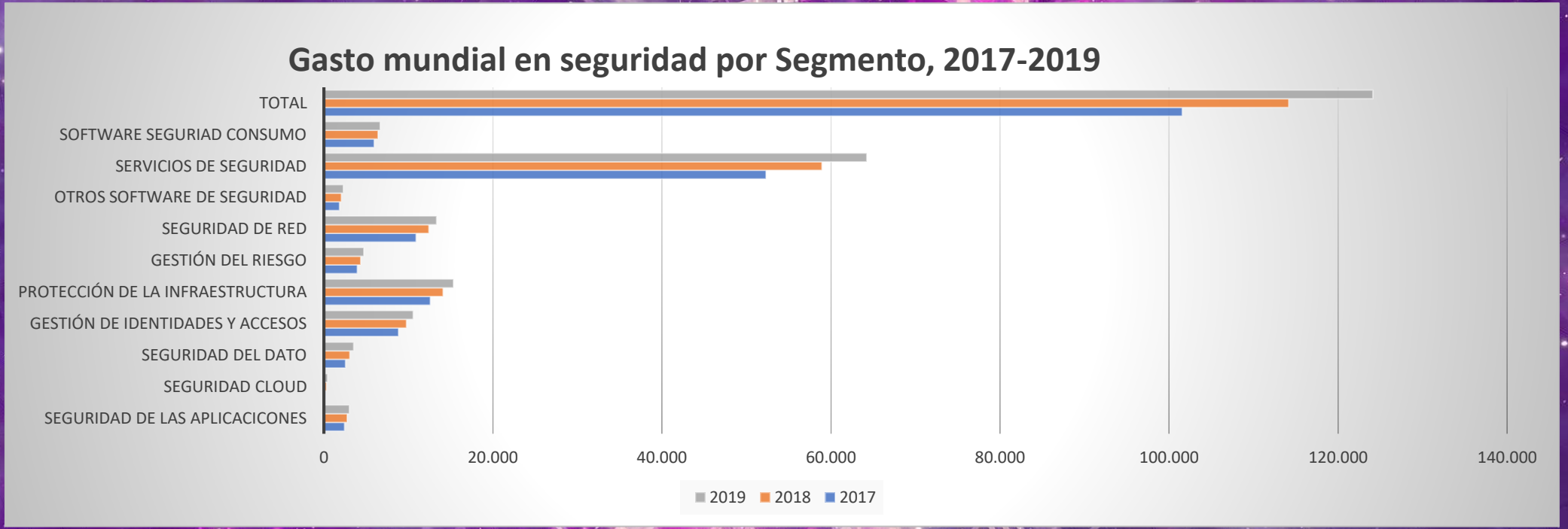

Predicciones de
Ciberseguridad 2019

Gartner prevé que el gasto en seguridad empresarial mundial alcanzará los 124.000 millones de dólares en 2019, un 8% más respecto a 2017.



"Las organizaciones están gastando más en seguridad como resultado de las regulaciones, la cambiante mentalidad de los compradores, el conocimiento de las amenazas emergentes y la evolución a una estrategia digital", Gartner

1 Ransomware, Cryptojacking y Fileless malware, líderes de amenazas

- **El fileles malware ya es el 35% del total de ataques registrados y para 2019 será el 50% de los ataques totales de malware.**
- **En 2018 el crecimiento del ransomware ha sido del 93% y los ataques a empresas aumentaron hasta un 90%.**
- **El número de variantes de malware de cryptojacking creció de 8 en 2017 a 25 en Mayo del 2018.**

Las campañas de ransomware dirigido causarán el caos en 2019 al centrarse en los sistemas de control industrial y los servicios públicos para obtener mayores beneficios. La demanda de pago medio aumentará en más del 6.500%, con una media de entre 300 a 20.000 dólares por ataque.

El pasado mes de noviembre Adguard reportó una tasa de crecimiento del 31% por ciento para el cryptojacking en el navegador. Su investigación encontró 33.000 sitios web que ejecutan scripts de minería criptográfica. Adguard estimó que esos sitios tenían 1.000 millones de visitantes mensuales combinados.

El malware sin archivos es más difícil de identificar y bloquear para la detección en los endpoints tradicionales porque se ejecuta íntegramente en memoria, sin dejar caer nunca un archivo en el sistema infectado.

2 La seguridad se centrará en el Dato

- **El mercado de seguridad global centrado en datos aumentará de 1.790 millones de dólares de 2016 a 5.830 millones para 2022, con un crecimiento medio anual del 23,1%.**

El perímetro desapareció con el cloud y la movilidad. Ahora el dato es la moneda de cambio, y hay que saber protegerlo. El mayor desafío es saber qué tipos de datos se almacenan, dónde se encuentran, quién tiene acceso a ellos y cómo se manejan. El descubrimiento continuo de datos será una necesidad en 2019 .

Las soluciones de seguridad centradas en los datos ayudan a las organizaciones a proteger los datos confidenciales en lugar de proteger la infraestructura de TI. Los componentes de seguridad centrados en los datos incluyen cifrado, administración de claves de cifrado, prevención de pérdida de datos, descubrimiento de datos y clasificación de datos, informes y auditorías, entre otros.

3 Analítica y Automatización

- **En 2017 menos del 1% de empresas con más de cinco profesionales de seguridad IT utilizaban herramientas de SOAR. Para 2020 el porcentaje habrá crecido hasta el 15%.**
- **El 62% de las empresas ya tiene procesos automatizados de respuesta a incidentes, y otro 35% está iniciando proyectos de SOAR o lo hará en los próximos 12 a 18 meses.**
- **El mercado SOAR crecerá desde los 826,1 millones de dólares en 2016 a 1.682 millones en 2021, con un crecimiento medio anual del 15.3%.**

Infraestructuras más complejas, cada vez más datos, regulaciones más estrictas y tecnologías como el cloud que deshacen el perímetro se han convertido en un problema que se suma a la falta de personal. Esto lleva a las empresas a buscar formas de automatizar los procesos de seguridad de TI, impulsando la demanda de soluciones que incorporen análisis avanzados, inteligencia artificial (AI) y tecnologías de aprendizaje automático (ML).

Los equipos de seguridad se enfrentan a más de 174.000 alertas por semana en promedio y solo pueden revisar alrededor de 12.000 de ellas. Alrededor del 62% de los encuestados mencionó la caza de amenazas como un beneficio esperado de SOAR (específicamente la automatización).

4 El riesgo de IoT sigue creciendo

- **El 20% de las compañías españolas ya ha desplegado proyectos reales de Internet de las Cosas y de éstas un 70% se está planteando ampliar estos proyectos en los próximos 18 meses, según IDC Research España.**

- **España es el quinto país en inversión en IoT en Europa, y se espera que el gasto crezca un 16% anualizado entre 2017 y 2021 alcanzado los 19.000 millones de euros.**

Los dispositivos conectados capaces de transmitir datos ya son parte del día a día, tanto en las empresas como en los hogares. Actualmente los dispositivos IoT son demasiado vulnerables y se espera que en 2019 los ciberdelincuentes inventen nuevos tipos de ataques contra el IoT. También se espera que los fabricantes presten más atención a la seguridad de los dispositivos.

Los botnets de la IoT seguirán creciendo a un ritmo imparable. Esto podría ser una advertencia recurrente año tras año, pero nunca debe subestimarse. A medida que las botnets de IoT continúen creciendo, pueden ser increíblemente poderosas en las manos equivocadas.

Se espera que el mercado de seguridad de IoT en general crezca de los 6.620 millones en 2017 a los 29.020 millones para 2022, con un crecimiento medio anual del 34,4% en el periodo.

5 Cumplimiento normativo, la asignatura aún pendiente

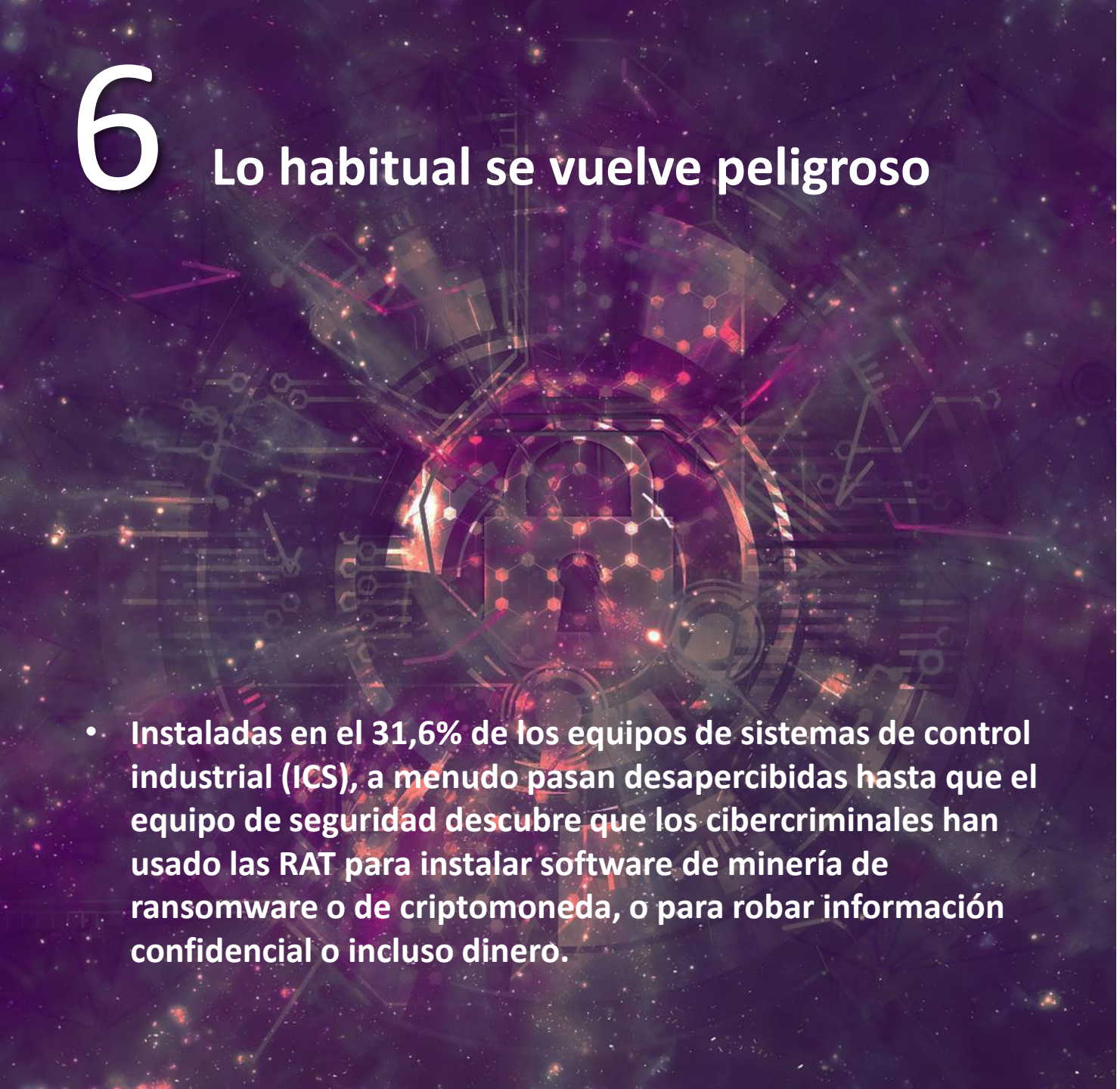
- **A dos meses de la entrada en vigor de GDPR la mitad de la pymes españolas no estaban familiarizadas con el reglamento.**
- **Más de un tercio reconocía que no estarían listas a tiempo.**
- **Y un 22% afirmaba no tener los recursos necesarios para adaptarse a esta nueva regulación.**

Desde 2018 directivas como GDPR o NIS son de obligado cumplimiento. A pesar de ello, son muchas las empresas que aún buscan la manera de ponerse al día. Por eso se prevé que el Cumplimiento como servicio se convierta en tendencia.

A mediados de este año el 85% de las empresas en Europa y Estados Unidos aún no estaba adaptada a los nuevos requerimientos de GDPR. Además, 1 de 4 compañías no ha completado su adecuación a ley incluso a finales de año.

Se prevé que para 2020, hasta el 75% de las nuevas aplicaciones empresariales tendrán que tomar la difícil decisión de elegir entre el cumplimiento y la seguridad.

6 Lo habitual se vuelve peligroso



- **Instaladas en el 31,6% de los equipos de sistemas de control industrial (ICS), a menudo pasan desapercibidas hasta que el equipo de seguridad descubre que los cibercriminales han usado las RAT para instalar software de minería de ransomware o de criptomoneda, o para robar información confidencial o incluso dinero.**

Que la mayor parte del malware se diseña para ejecutarse exclusivamente para ordenadores Windows no es nuevo.

Lo que sí parece más novedoso y se convierte en tendencias es que los ciberdelincuentes estén abusando de las herramientas de administración legítimas en el sistema operativo de Windows (SO), como PowerShell, WMI y Windows Scripting Host, para evadir la detección y generar nuevas oleadas de ataques.

Los atacantes no muestran signos de renunciar a nuevas variaciones en los ataques de macros de Microsoft Office, otra ruta para lanzar ataques sin la necesidad de ejecutables convencionales

Las herramientas legítimas de administración en remoto (RAT) representan una seria amenaza para las redes industriales.

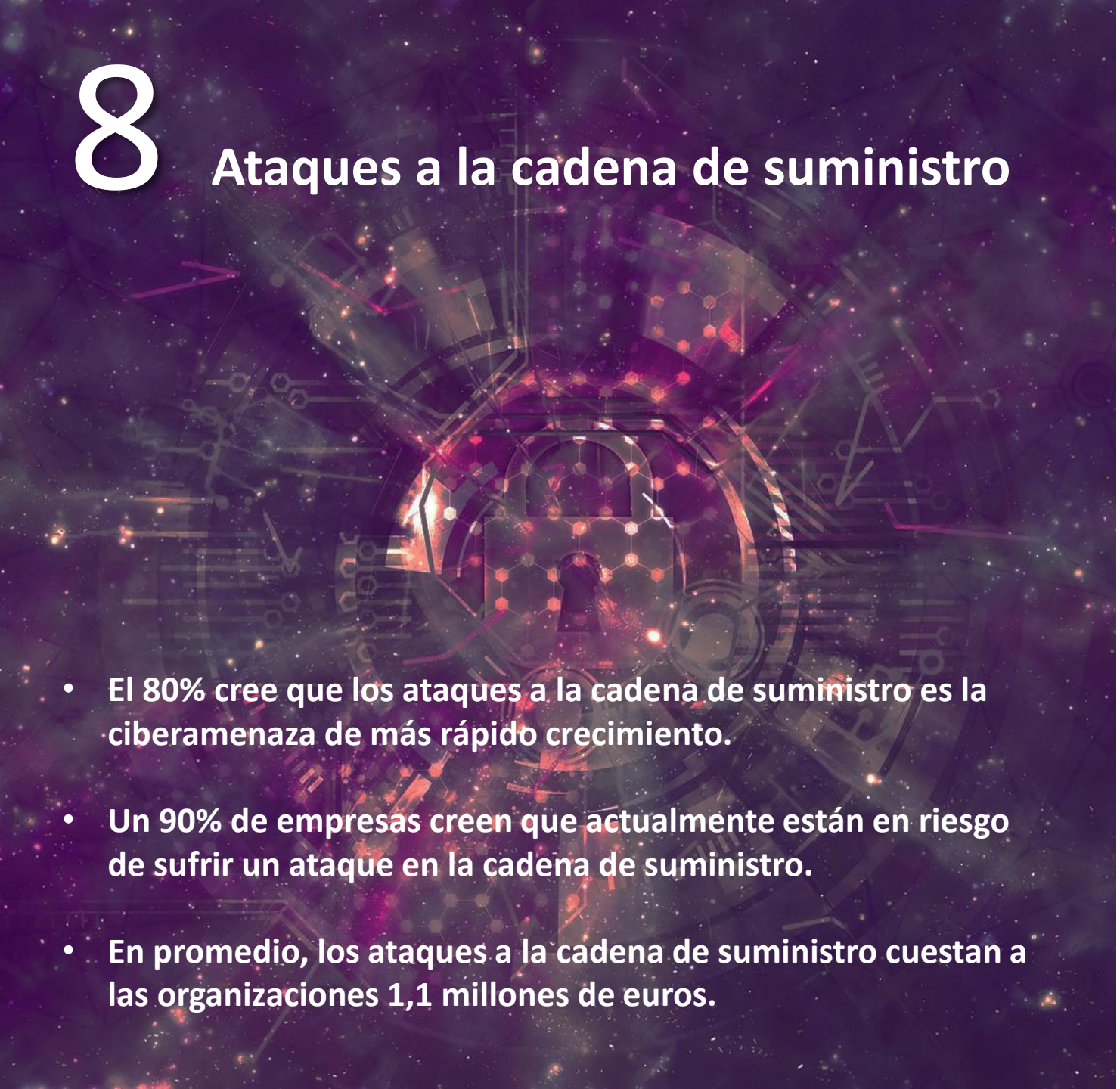
7 Seguridad biométrica, apuesta segura

- **El mercado global de la biometría superará los 50.000 millones de dólares para el 2024, convirtiéndose en uno de los mercados tecnológicos más prometedores.**
- **La comercialización de sensores de huellas digitales llegará a cerca de dos mil millones en el año 2021, con una tasa de crecimiento global del 44%.**

Las empresas usarán herramientas biométricas sencillamente porque aumentan de manera significativa la efectividad de las prácticas de seguridad. Y a medida que se avance en su uso e implantación, la integración de la experiencia del usuario mejorará, mientras que el estigma asociado con las huellas dactilares o los escaneos faciales se disipará al mismo tiempo.

Según la consultora ABI Research la seguridad biométrica alcanzará los 30.000 millones en 2021, un crecimiento del 118% respecto a 2015.

8 Ataques a la cadena de suministro



- **El 80% cree que los ataques a la cadena de suministro es la ciberamenaza de más rápido crecimiento.**
- **Un 90% de empresas creen que actualmente están en riesgo de sufrir un ataque en la cadena de suministro.**
- **En promedio, los ataques a la cadena de suministro cuestan a las organizaciones 1,1 millones de euros.**

Se trata de uno de los vectores de ataque más preocupantes que se ha explotado con éxito durante los últimos dos años. Este tipo de ataque hizo que todos pensaran en la cantidad de proveedores con los que trabajan y qué tan seguros están.

El 87% de los encuestados sufrieron un ataque de la cadena de suministro de software.

Un 80% de los responsables de TI creen que los ataques a la cadena de suministro tienen el potencial de convertirse en una de las mayores ciberamenazas en los próximos tres años.

El 71% cree que su organización no siempre mantiene proveedores externos con los mismos estándares de seguridad

9 Blockchain y la ciberseguridad

- **Se prevé que el mercado mundial de blockchain alcanzará un valor 20.000 millones para 2024, según Transparency Market Research.**
- **Nuevas e innovadoras soluciones basadas en blockchain podrían aprovecharse de una industria de 27.200 millones de**
- **dólares.**

El impacto de Blockchain es enorme en el entorno financiero, pero también tiene un gran potencial para el mercado de seguridad. Entre sus ventajas, que todo lo que ocurre en la cadena de bloques está cifrado e impide la alteración del dato.

La seguridad basada en blockchain no será ampliamente adoptada en 2019, pero empezaremos a ver su penetración, por lo que conviene estar familiarizados con esta tecnología.

Según Panda Security, “hay quien se atreve a comparar el blockchain con los servicios ofrecidos por los servidores DNS. Debido a la inviolabilidad del blockchain y su descentralización, si esta tecnología se usase para sustituir el sistema de nombre de dominio los ataques de denegación de servicio (más conocidos como DDoS) serían imposibles”.

10 La contrainteligencia gana posiciones

- **El mercado de inteligencia de amenazas crecerá una media anual del 18,1% entre 2018 y 2023.**
- **Cuatro de cada cinco empresas asegura que el threat hunting será prioritario en sus iniciativas de seguridad el próximo año.**

Las empresas buscarán nuevas herramientas y nuevas formas de engañar a los atacantes para que vayan a donde se les pueda observar, hacer un perfil y saber lo que buscan.

Del 60% de las empresas que utilizan técnicas de threat hunting aseguran que la búsqueda de amenazas proporcionó una mejora medible en la seguridad de sus organizaciones.

El 50% de los encuestados dijo que una inversión en una plataforma de búsqueda de amenazas se amortiza en un año dada su capacidad para detectar amenazas desconocidas, emergentes y avanzadas.

CON LA COLABORACIÓN DE: