Channel Futures

CIBERPROTECCIÓN Y COPIA DE SEGURIDAD EN LA NUBE

La forma más fácil para los VAR de generar ingresos por servicios

POWERED BY | Acronis

INTRODUCCIÓN

Hoy en día el cambio es la nueva norma. La potencia imparable de la transformación digital continúa redefiniendo prácticamente todas las etapas y facetas del comercio mundial, incluido el segmento de los distribuidores de valor añadido (VAR). El modelo de VAR está atravesando una reconversión radical impulsada por fuerzas que incluyen la nube, el crecimiento exponencial de dispositivos y datos, una variedad cada vez mayor de soluciones de software como servicio (pensadas para una variedad cada vez mayor de fórmulas de negocio) y las innovaciones en automatización, fuerzas que cuestionan qué papel cumplen los VAR y cómo se definirá su éxito en la próxima década.

Merecen reconocimiento los VAR con visión de futuro que se adaptan a estos cambios profundos, aunque lo hagan despacio. Muchos han añadido licencias periódicas, soluciones SaaS e infraestructura en la nube a su cartera de productos, un paso importante en la dirección correcta.

Pero aún queda mucho por hacer en un mundo donde las organizaciones claramente prefieren alquilar servicios de TI de proveedores especializados a comprar y manejar tecnologías internamente. En este entorno competitivo se están multiplicando las nuevas empresas que ofrecen "todo como servicio" y reinventan las tácticas de comercialización a una velocidad vertiginosa. Los VAR deben evolucionar a la par, pues de lo contrario...

Como demuestran las páginas que siguen, el camino más directo para que un VAR tenga éxito y crecimiento duraderos está en adoptar la estrategia "como servicio", cada vez más lucrativa, para ofrecer servicios de protección de datos y copia de seguridad en la nube. A partir de 2020, les irá mejor a los que sepan gestionar un número creciente de servicios en la nube, aprovechar las herramientas de automatización para atender a sus clientes y estudiar sin descanso nuevas formas de maximizar las numerosas plataformas que surjan en el ecosistema tecnológico, incluidas las que presenten ofertas de automatización con las que puedan prestar con eficacia servicios de más valor. También hay nuevas plataformas de servicios gestionados que se encargan de aspectos operativos fundamentales, actualizaciones de seguridad, gestión de la infraestructura y tareas rutinarias.

Adoptando la plataforma adecuada y una lista escogida de soluciones, los VAR pueden ofrecer servicios gestionados a sus clientes y sus partners sin las dificultades y los gastos que conlleva el desarrollo de un modelo o unidad de negocio enteramente nuevo. Veamos cómo.

Argumentos comerciales para añadir servicios de más valor

Hay varios motivos de peso para que los VAR amplíen su oferta de servicios gestionados y de servicios periódicos de más valor. Algunos —como la estabilidad y la previsibilidad que aportan al negocio unos ingresos fijos frente a las compras esporádicas, así como una mayor rentabilidad— son bastante obvios.

Sin embargo, lo más importante es que los VAR que mantengan el rumbo y ofrezcan únicamente las tradicionales renovaciones de licencia, contratos de mantenimiento y soporte, y servicios gestionados básicos serán cada vez más vulnerables. Ofrecer servicios en la nube protege a los VAR de la obsolescencia: la nube es el segmento de servicios de TI de más rápido crecimiento. Gartner prevé que, a medida que las empresas abandonen los servicios tradicionales y adopten la mentalidad "cloud-first" a la hora de seleccionar productos y servicios de TI[i], el mercado mundial de servicios en la nube pública pasará de 182 400 millones de USD en 2018 a 331 200 millones en 2022[ii].

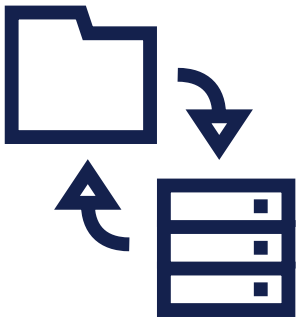
Servicios de TI: Los 5 MEJORES y los 5 PEORES

por % de TCAC (2017-2022)

Fuente: seminario web de Gartner; Top Trends Driving Change for IT Services (Principales tendencias que impulsan el cambio en los servicios de TI)

Los 5 mejores	% de TCAC 2017-2022
IaaS	**26,6**
Servicios básicos para infraestructuras	**14,1**
Móviles (Servicios gestionados para centros de trabajo)	**11,3**
Coubicación	**11,0**
Alojamiento	**10,4**

Los 5 peores	% de TCAC 2017-2022
Sobremesa (Servicios gestionados para centros de trabajo)	**–3,5**
Asistencia para hardware (Asistencia para dispositivos del cliente)	**–3,4**
Externalización del servicio de asistencia	**–3,2**
Externalización del centro de datos	**–2,5**
Externalización de la red empresarial	**–2,3**



El sector de servicios gestionados en la nube tampoco es ajeno al crecimiento exponencial: a ritmo similar, este mercado mundial tiene visos de alcanzar 84 700 millones de USD para 2023, cifra que duplica con holgura los 41 400 millones de 2018[iii]. Según Gartner, los servicios relacionados con la nube, como asesoría, consultoría, implementación, migración y servicios gestionados, sumarán el 28 % de los presupuestos totales para la nube en 2022[iv].

Conclusión: los VAR que deseen mejorar sus resultados tanto a medio como a largo plazo deberán incrementar su cartera de servicios gestionados en la nube. El mundo está adoptando la nube, y los VAR que no se suman a esta tendencia quedan relegados.

Creación y gestión de una cartera de servicios en la nube

¿Cómo pueden los VAR dar el salto? Los servicios gestionados en la nube se basan en dos elementos fundamentales. El primero es una **plataforma** para la gestión, contratación, integración y personalización de los servicios.

Crear una plataforma de gestión de servicios supone un esfuerzo enorme y complejo de desarrollo de software, de ahí que para los VAR (así como los MSP, o proveedores de servicios gestionados) sea más conveniente trabajar con un socio tecnológico que les facilite una solución preconfigurada robusta y comprobada, por ejemplo **Acronis Cyber Cloud**. Una plataforma de servicios optimizada por el proveedor permite a los partners y a los VAR crear rápidamente paquetes de servicios en la nube con escasos o nulos costes iniciales; en las mejores plataformas es posible crear servicios diferenciados, ajustar modelos de negocio y de precios e integrar en la cartera los servicios en la nube.

Sea cual sea el proveedor, una plataforma de servicios gestionados en la nube debe ofrecer las siguientes funciones:

- Capacidad multiinquilino con separación segura de servicios para atender a múltiples clientes
- Posibilidad de crear varias ofertas y paquetes de servicios
- Inicio de sesión único para cuentas de clientes e integración en sistemas SSO externos

- Un motor de directivas que admita directivas de uso y seguridad personalizadas, como los controles de acceso basados en la función (RBAC)
- Cuotas de uso
- Varios modelos de pago, como pago por uso, suscripción anual, capacidad reservada, etc.
- Una consola de administración unificada compatible con entornos multiinquilino
- Amplios informes de uso, auditoría, indicadores y paneles
- Integración en otros sistemas, lo que incluye aprovisionamiento de usuarios, autenticación de usuarios/gestión de identidades y accesos, facturación/cuentas por pagar, incidencias/asistencia y CRM
- Imagen de marca personalizada (es decir, oferta de marca blanca)
- Una API REST que facilite el desarrollo y la integración de servicios personalizados basados en la nube

El éxito de los servicios gestionados en la nube también se fundamenta en una estudiada **selección de servicios**. Por supuesto, un VAR puede seguir vendiendo cientos de soluciones de cientos de proveedores. Pero es mucho más razonable simplificar e identificar una serie de proveedores que satisfagan todas sus necesidades, o sea, proveedores de nichos especializados (p. ej., conexión en red, protección de datos, IaaS, gestión de infraestructuras, herramientas de productividad, etc.) que ofrezcan servicios imprescindibles como:

- Endpoints (equipos de sobremesa, portátiles y dispositivos móviles)
- Servicios de Internet y datos móviles
- Servicios de VOIP
- Impresoras
- Aplicaciones de correo electrónico y productividad para oficinas (Office 365 o Google Apps)
- Aplicaciones CRM
- Aplicaciones financieras
- Aplicaciones ERP/HCM
- Aplicaciones de marketing
- Administración de endpoints (móviles y de sobremesa/portátiles)

Acronis es una auténtica "navaja suiza" cuando se trata de ciberprotección. No cubre el cien por cien de las necesidades de servicios en la nube —ningún proveedor lo hace—, pero sí buena parte de ellos, incluidos:

- Servicios de protección de datos
- Continuidad de la actividad empresarial
- Soluciones de seguridad para endpoints (p. ej., protección contra el ransomware)
- Almacenamiento y uso compartido de archivos
- Servicios de certificación, verificación y firma digital de archivos

Independientemente de los sectores verticales que decida atender un VAR, hay soluciones de Acronis que añadirán valor a sus clientes.

Protección de datos: la base de una cartera de servicios en la nube

Como estrategia de negocio, siempre es saludable buscar categorías de productos y servicios con un gran mercado total disponible, y la protección de datos como servicio (DPaaS, por sus siglas en inglés) reúne todos requisitos. IDC prevé que este mercado crecerá con una TCAC del 16,2 % hasta 2022, cuando alcanzará 10 200 millones de USD[v].

Una cartera atractiva de servicios de protección de datos empieza por ofrecer una **copia de seguridad de confianza** de los datos en servidores y matrices de almacenamiento empresariales tradicionales, pero también en máquinas virtuales, entornos de almacenamiento virtual y recursos basados en la nube. Un producto como **Acronis Cyber Backup Cloud** permite a los VAR almacenar de forma segura todos los activos de datos fundamentales de una organización con una estructura híbrida que admita tanto el almacenamiento local como el almacenamiento en la nube, y que no obligue a los clientes a limitarse a un solo lugar o entorno.

Los servicios de **recuperación ante desastres (RD)**, otro componente indispensable de una oferta exhaustiva de protección de datos, complementan la copia de seguridad con la capacidad de recuperar datos rápidamente y reiniciar aplicaciones en infraestructuras secundarias (normalmente un sitio de recuperación de datos en la nube).

La automatización de procesos que suele necesitar un servicio de recuperación ante desastres a prueba de fallos puede exigir un esfuerzo considerable de desarrollo de software, algo que los VAR pueden eludir con un producto SaaS como **Acronis Cyber Disaster Recovery Cloud**, que añade la recuperación ante desastres a su cartera de servicios en la nube. Este producto, que se suministra listo para su uso, admite cargas de trabajo físicas y virtuales, contiene un editor de GUI para crear automatizaciones de RD y puede ensayar varios casos de recuperación sin interrumpir los sistemas de producción.

A continuación, las características de **sincronización, uso compartido y almacenamiento de archivos** cubren las funciones de intercambio de archivos en la nube que demandan las empresas, acompañadas de seguridad, controles empresariales y protección de datos. Aunque algunos servicios para particulares ofrecen versiones empresariales, en general se trata de productos independientes que no encajan bien con otros servicios de seguridad y protección de datos que utilizan las empresas. Por su parte, los VAR pueden ofrecer una solución completa e integrada incorporando **Acronis Cyber Files Cloud**, un servicio personalizable que funciona con sistemas de almacenamiento existentes o con la infraestructura en la nube de Acronis. Al igual que los servicios para particulares, admite dispositivos móviles, PC de Windows, equipos Mac y todos los navegadores web más utilizados, pero también incluye funciones de corte empresarial, como edición in situ para documentos de Microsoft Office.

A estas propiedades se suman las imprescindibles para una oficina virtual: las funciones de **certificación, verificación y firma digital de archivos** ofrecen un mecanismo seguro e irrefutable para aprobar documentos electrónicos y validar su autenticidad. Un producto SaaS como **Acronis Cyber Notary Cloud** permite a los VAR ofrecer un servicio basado en blockchain para certificar, verificar y firmar archivos electrónicamente, y hace posible que los clientes autentiquen documentos importantes y satisfagan los requisitos normativos de transparencia e integridad de los datos.

Y, hablando de estrategias comerciales saludables, los servicios de protección de datos demuestran reiteradamente ser **la venta más fácil que puede hacer un proveedor de tecnología**. De hecho, muchos de los mayores MSP actuales empezaron ofreciendo soluciones de copia de seguridad, recuperación ante desastres y protección; después se posicionaron y expandieron a partir de ahí.

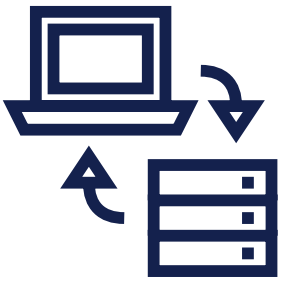
Más allá de la protección de datos para mantener la competitividad

Está claro que las dificultades tradicionales, como las interrupciones del suministro eléctrico y los desastres naturales, no son los únicos riesgos a los que se enfrentan las empresas del siglo XXI. Las ciberamenazas suponen un gran peligro para las organizaciones de todo el mundo. Según Accenture[vi], las violaciones de seguridad digital han crecido un 67 % en los últimos cinco años, un 11 % solo en el último año.

Es una mala noticia para las empresas, pero no para los VAR. En un mundo donde se pierden 2,9 millones de USD al minuto por la ciberdelincuencia[vii], los VAR ganan una importante ventaja competitiva cuando evolucionan desde los productos básicos tradicionales a una ciberprotección exhaustiva. Acronis describe la ciberprotección como una nueva generación de protección de datos que converge con la ciberseguridad y la trasciende al abarcar los cinco vectores de lo que denomina **SAPAS**. Los VAR pueden crear servicios de protección de datos seguros y diferenciados para sus clientes basándose en estos componentes.

La sigla SAPAS empieza por la **salvaguarda**, que consiste en asegurar que siempre haya copias no adulteradas de los datos. También contempla la **accesibilidad**, para que los clientes y los empleados siempre conectados de hoy en día puedan acceder y utilizar los datos corporativos desde cualquier lugar, así como las medidas de **privacidad**, para garantizar que los datos confidenciales y sensibles queden a salvo de la mirada indiscreta de personas no autorizadas (y a la vez facilitar los controles necesarios para los usuarios legítimos). No menos crucial es la **autenticación**, que asegura que los datos no se hayan modificado clandestinamente y que las copias legítimas sean idénticas al original.

Por último, pero sin duda de igual importancia, los VAR deben ofrecer soluciones de **seguridad** para proteger datos, sistemas y usuarios frente a los agentes maliciosos, tanto hackers externos como empleados no autorizados. La seguridad debe cubrir tanto los datos en reposo (almacenados) como en tránsito (en la red) mediante diversas técnicas, como cifrado, hash, firmas digitales, supervisión y prevención y corrección de ataques.



Los VAR y los MSP que ofrezcan un conjunto integrado de servicios seguros de protección de datos también deberán tener en cuenta la protección contra el ransomware. Se calcula que, para finales de 2019, el ransomware (un tipo de malware que bloquea el acceso a sistemas y datos informáticos y solo restablece el acceso cuando el propietario paga un rescate a los agresores) atacará a una empresa cada **14 segundos**[viii]. Según un informe de Malwarebytes, los ataques a objetivos empresariales ya han aumentado un 195 % entre el cuarto trimestre de 2018 y el primer trimestre de 2019[ix].

Acronis Active Protection impide que el ransomware cifre e inhabilite archivos, copias de seguridad e incluso el propio software de copia de seguridad, y vigila constantemente los accesos y las modificaciones de archivos para identificar y detener las actividades potencialmente peligrosas antes de que un ataque cause estragos. Y, en caso de que el ransomware logre atravesar las defensas, Acronis Active Protection restablece automáticamente los archivos cifrados, lo que ahorra un tiempo enorme a los proveedores de servicios en la recuperación y la reducción del tiempo de inactividad. Al estar integrada en Acronis Cyber Backup Cloud, esta tecnología reduce de forma instantánea su exposición y la de sus clientes al ransomware sin necesidad de instalar nada sobre sus agentes de copia de seguridad.

Ciberprotección con Acronis

Acronis Cyber Cloud no se limita a ofrecer soluciones de copia de seguridad, recuperación ante desastres, sincronización y uso compartido de archivos, certificación de documentos y seguridad de los datos. También se integra en las principales herramientas administrativas de MSP/CSP (proveedores de servicios en la nube) —por ejemplo, administración de servicios, incidencias, supervisión y alertas— para aumentar la eficacia de los MSP.

Además, Acronis Cyber Cloud es la *única* solución que ofrece un conjunto de servicios de ciberprotección muy demandados y una plataforma de aprovisionamiento y administración de usuarios, lo que otorga a los proveedores de servicios la libertad de promocionar su propia marca y tratar directamente con sus clientes. Acronis Cyber Cloud también brinda acceso a la infraestructura en la nube y la asistencia a sistemas privados de Acronis para la prestación de servicios.

Planificación para partners: cómo empezar a vender Acronis Cyber Cloud

Si crea su cartera sobre la sólida base SaaS de un proveedor de software consolidado, un VAR puede ofrecer servicios en la nube con una **inversión inicial mínima en tiempo y dinero** junto con el respaldo de un socio con profunda experiencia en protección de datos de confianza.

Además de experiencia técnica, un proveedor de servicios en la nube debe ofrecer asistencia exhaustiva de ventas y marketing a través de su programa de partners. Los expertos del programa de Acronis para partners Cloud ayudan a los VAR en todas las etapas del proceso de prestación de servicios, desde el arranque (cuando Acronis ayuda a los VAR con los trámites de inicio del servicio, establecimiento de precios y desarrollo de paquetes) hasta la incorporación de clientes, las campañas periódicas de marketing y la asistencia preventas.

Servicios de protección de datos de confianza: ejemplos y casos de uso

Las funciones de protección de datos de confianza que ofrece Acronis Cyber Cloud permiten a los VAR comercializar una gran cantidad de servicios en la nube, genéricos y personalizados, concebidos para atraer a organizaciones de todas las formas y tamaños. Las categorías más utilizadas incluyen:

Servicios de protección de datos híbridos multifacéticos que funcionan en cualquier infraestructura, incluidos servidores o matrices de almacenamiento locales, sistemas gestionados por el VAR en una coubicación o recursos de almacenamiento en la nube. En una implementación típica, los servicios en la nube se emplean como archivo de almacenamiento principal, pero se mantienen copias secundarias opcionales en espacios de almacenamiento local. Estas implementaciones híbridas permiten a los VAR prestar el servicio en la nube y realizar ventas cruzadas de paquetes de hardware-software para gestionar el almacenamiento local.

La creciente popularidad de las aplicaciones SaaS, como Office 365, presenta otra situación ideal para proponer servicios en la nube utilizando una solución como Acronis Cyber Backup Cloud. Ahora numerosos VAR ofrecen un **paquete de Office 365 con una solución de copia de seguridad,** que ayuda a sus clientes a satisfacer sus objetivos de protección de datos y, en algunos casos, sus requisitos normativos.

Los servicios SaaS de protección de datos pueden ampliarse con **sincronización y uso compartido de archivos en la nube** para incrementar la colaboración sin dejar de controlar las filtraciones de datos y los accesos no autorizados.

Los **servicios de recuperación ante desastres basados en la nube** complementan los servicios de archivo de datos con la automatización de procesos para restablecer las operaciones interrumpidas en las ubicaciones remotas que gestiona el proveedor, lo que elimina la necesidad de infraestructura redundante y costosa en la organización. Desde una perspectiva a largo plazo, a medida que los clientes adopten la infraestructura en la nube para alojar aplicaciones empresariales, los VAR podrán ampliar el servicio para utilizar recursos IaaS como ubicación de recuperación ante desastres.

Los **servicios convergentes de protección de datos y seguridad** combaten la lacra del ransomware, que secuestra los valiosos datos de la organización. Esta inutilización de los datos demuestra la insuficiencia de las defensas tradicionales basadas en malware y subraya la necesidad de combinar la protección de datos y la supervisión de la seguridad bajo un paraguas de servicios simbióticos. Muchas soluciones antivirus tradicionales basadas en firmas han perdido capacidad defensiva. Ahora son las soluciones más modernas de protección de datos con tecnología como Acronis Active Protection,

que recurre a sofisticados modelos de aprendizaje automático para detectar y detener el ransomware, las que permiten que los VAR y los MSP ofrezcan servicios de seguridad avanzados dejando la complejidad de su implementación y su gestión a un experto externo.

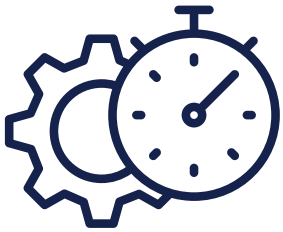
Los partners y los VAR también pueden ampliar y personalizar estos servicios básicos genéricos con funciones destinadas a sectores y clientes concretos. Con una plataforma ampliable y de marca blanca como la suite Acronis Cyber Cloud, los partners tienen garantizado el control absoluto de su marca, su personalización y la relación con sus clientes. Los VAR y los MSP pueden ampliar las funciones de la suite **Acronis Cyber Cloud** con Acronis Cyber Platform, que ofrece distintos API y SDK; además, las posibilidades de personalización y ampliación les permiten crear ofertas únicas para diferenciar su marca de la competencia.

Los servicios específicos tienen buena acogida en el ámbito de la **copia de seguridad de estaciones de trabajo en la nube**, así como en el de **archivado a largo plazo con almacenamiento en bóveda** y servicios más económicos de almacenamiento inactivo en la nube para cumplir las normativas.

Otra oportunidad de prosperar está en el **sector sanitario**, donde el almacenamiento y las copias de seguridad deben cumplir con la norma HIPAA. **Un MSP especializado en servicios para dentistas** utilizaba el cifrado AES-256 incorporado de Acronis Cyber Backup Cloud para ofrecer un servicio conforme con HIPAA y ahorrar 30 000 USD frente al anterior software de copia de seguridad. Y, tras migrar a Acronis Cyber Backup Cloud, **un importante proveedor de soluciones de gestión de prácticas automatizada e historias clínicas electrónicas** redujo un 90 % el tiempo de recuperación y multiplicó por diez su base de clientes en dos años al aprovechar la escalabilidad de los servicios en la nube.

Otra propuesta irrenunciable más: la ciberprotección dirigida a los sectores verticales de **venta minorista, logística y seguros**, unos sectores con redes distribuidas de oficinas que cuesta administrar y proteger de forma centralizada. A este tipo de empresas, la plataforma de Acronis les ofrece:

- Ciberprotección centralizada para todas las sucursales, con directivas de copias de seguridad centralizadas y autoservicio de recuperación
- Funciones de recuperación remota, incluida la recuperación remota automatizada centralizada



- Automatización de recuperación con un clic sin necesidad de personal de TI
- Sin inversión en bienes de equipo en las oficinas: todos los servicios se ejecutan en la nube
- Panel único de administración para servidores, estaciones de trabajo y Office 365

Recomendaciones y llamada a la acción

Los servicios de protección de datos de confianza en la nube ofrecen a los VAR importantes oportunidades para aumentar ingresos fijos y márgenes, así como para sorprender y conservar a sus clientes. Si se asocian con un proveedor de software consolidado como Acronis para crear una cartera de servicios, los VAR pueden centrarse en lo que importa: con Acronis de su lado, pueden concentrar su energía en **diferenciar y personalizar** sus servicios y en **mejorar sus márgenes con menos gastos generales**. También pueden **abordar amenazas nuevas y cambiantes como el ransomware, agilizar el desarrollo y la implementación de servicios** y **conseguir ventas cruzadas de productos y servicios afines.** Y sobre todo, los VAR pueden **desarrollar una marca fuerte con la que granjearse la fidelidad de los clientes y reducir su rotación.**

Póngase en contacto con el departamento comercial de Acronis para hablar de su negocio y ver una demostración de productos.

CONTÁCTENOS >

Fuentes

[i] Gartner. "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019" (Gartner prevé un aumento del 17,5 % en los ingresos de la nube pública en 2019). Nota de prensa, 2 de abril de 2019.

[ii] Gartner. "Top Trends Driving Change for IT Services" (Principales tendencias que impulsan el cambio en los servicios de TI). Seminario web, 25 de marzo de 2019.

[iii] IDC. "Worldwide Managed Cloud Services Forecast, 2019–2023: An Extraction View of Technology Outsourcing Services Markets" (Previsión mundial sobre servicios gestionados en la nube, 2019-2023: análisis de los mercados de servicios de externalización tecnológica). Predicción de mercado, septiembre de 2019.

[iv] Prabha, Anil. "Public Cloud Services Market to Hit $214bn" (El mercado de servicios en la nube pública alcanzará los 214 000 millones de USD). TechHQ, 8 de abril de 2019.

[v] IDC. "Worldwide Data Protection as a Service Forecast, 2018–2022: Initial Market Sizing" (Previsión mundial sobre la protección de datos como servicio, 2018-2022: dimensiones iniciales del mercado). Predicción de mercado, julio de 2018.

[vi] Accenture. Ninth Annual Cost of Cybercrime Study (Noveno estudio anual sobre el coste de la ciberdelincuencia), 6 de marzo de 2019.

[vii] "Cybercrime Costs Global Economy $2.9m Per Minute" (Los costes de la ciberdelincuencia para la economía mundial suman 2,9 millones de USD por minuto). Infosecurity Magazine, 24 de julio de 2019.

[viii] Morgan, Steve. "Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019" (Los costes mundiales de los daños del ransomware alcanzarán los 11 500 millones de USD en 2019). Cybercrime Magazine, 17 de noviembre de 2017.

[ix] Zamora, Wendy. "Cybercrime Tactics and Techniques Report Finds Businesses Hit with 235 Percent More Threats in Q1" (Un informe sobre las técnicas y las tácticas de la ciberdelincuencia concluye que las empresas han recibido un 235 % más de amenazas en el T1). MalwareBytes Labs, 25 de abril, 2019.