EM ESTUDIO DE MERCADO

2021

ICEX España Exportación e Inversiones

El mercado de la ciberseguridad en Argentina

Oficina Económica y Comercial
de la Embajada de España en Buenos Aires

EM ESTUDIO DE MERCADO

30 de junio de 2021
Buenos Aires

Este estudio ha sido realizado por
Alejandro Cobelo Pardo de Donlebun

Bajo la supervisión de la Oficina Económica y Comercial
de la Embajada de España en Buenos Aires

http://argentina.oficinascomerciales.es

Editado por ICEX España Exportación e Inversiones, E.P.E.

NIPO: 114-21-009-9

Índice

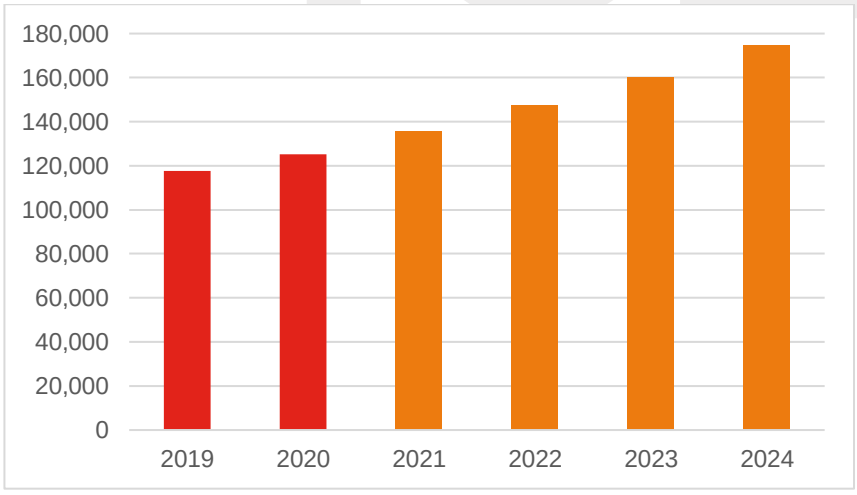
1. Resumen ejecutivo

El principal objetivo de este estudio es analizar el sector de la ciberseguridad en Argentina. Para ello, a partir de los datos recogidos en diversas fuentes, se ofrece información sobre la evaluación de su oferta y demanda — con enfoque en sus características y tendencias —, las barreras de entrada al mercado y las posibilidades de generar negocio en el mismo.

En un mundo cada vez más dependiente de la tecnología, la seguridad cibernética se ha convertido en una herramienta fundamental y prioritaria para la defensa, no solo de las instituciones públicas y la empresa privada, sino también de la sociedad civil.

Como consecuencia de la pandemia, su importancia es cada vez mayor, pues millones de trabajadores se han visto forzados a trabajar desde sus casas, con equipos desprotegidos, lo que ha generado que la frecuencia de los ciberataques haya aumentado y, por ende, también su impacto económico: para este año, se estima que las pérdidas alcancen los 6 billones de dólares.

Asimismo, el tamaño del mercado mundial creció un 6 % durante el año pasado y se proyecta que para 2024, su cifra se aproxime a los 175.000 millones de dólares.

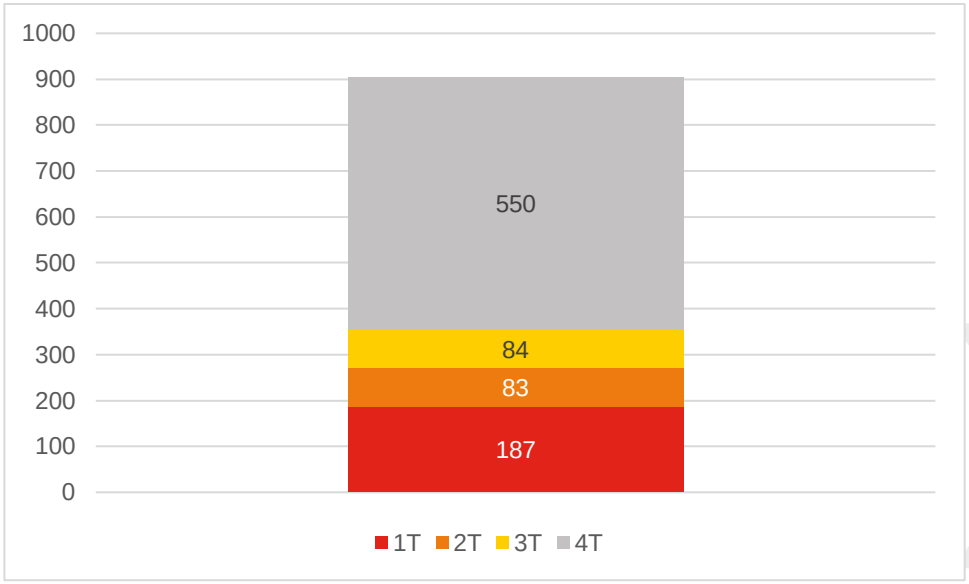


Fuente: elaboración propia a partir de IDC

Por su parte, la implantación de la ciberseguridad en Argentina, todavía se encuentra en su etapa inicial de madurez — por detrás de los mercados referentes del sector —; sin embargo, y a pesar de las dificultades derivadas por las constantes fluctuaciones del tipo de cambio y la devaluación de su moneda oficial, las diversas medidas adoptadas en los últimos años — legislativas y educativas — han afectado de manera positiva al sector.

Igualmente, la realidad actual es que Argentina ha obtenido una puntuación de 50,12 en materia de seguridad cibernética, y se sitúa en la posición 91 — de 194 naciones — del ranking mundial elaborado por la International Telecommunication Union (ITU).

Con relación a los datos registrados el año pasado, el número de ataques cibernéticos fue 904 millones — la mayoría en el último trimestre del año — y la principal modalidad fueron las campañas de *phishing*: 4.509 diarias



Fuente: elaboración propia a partir de Fortinet

Por otro lado, el 65 % de las principales empresas privadas del país sufrieron al menos uno y, de estas, un 40 % considera que será víctima de otro a lo largo de 2021. Por su parte, el sector más afectado fue el financiero, especialmente la banca privada.

Este gran margen de mejora ofrece un abanico de oportunidades en un mercado fragmentado en el que compiten muchas pequeñas empresas nacionales y unas pocas que son líderes a nivel mundial.

Igualmente, para que estas puedan alcanzarse, es importante contar con el apoyo de la Administración Pública. En este sentido, la aprobación de la Estrategia Nacional de Ciberseguridad o la Ley de Economía del Conocimiento, han contribuido a afianzar el compromiso cibernético adoptado por el país hace unos años.

Por último, la empresa española interesada en el mercado argentino debe tener en cuenta que, además de la notable percepción local por los productos y servicios tecnológicos del país, existen acuerdos de colaboración en materia cibernética para la internalización del sector.

En suma, se trata de un rubro prometedor en un mercado particular como es el argentino: de gran tamaño y relevancia en Latinoamérica, pero complejo por la dificultad para desarrollar proyectos a medio y largo plazo debido a los ciclos de su economía y política.

2. Definición del sector

2.1. Definición de ciberseguridad

En los últimos años, el número de amenazas y ataques cibernéticos ha aumentado de forma significativa debido al rápido proceso de digitalización que se produce en la sociedad actual; empresas, instituciones y particulares cada vez más dependientes de un dispositivo tecnológico como resultado de la continua transformación de los procesos analógicos.

Consecuentemente, se ha creado cierta conciencia entre los usuarios respecto a la importancia de proteger la sensible información que se genera y comparte en el mundo digital. Además, el número de estas amenazas es cada vez mayor, así como su complejidad para detectarlas.

Es por todo esto, por lo que la ciberseguridad está más presente en nuestro día a día, tanto en el ámbito cotidiano como en el empresarial. Ahora bien, ¿a qué nos referimos cuando hablamos de ciberseguridad?

Es importante aclarar esto, pues a menudo se emplea el término «seguridad de la información» como sinónimo de «ciberseguridad» de forma errónea. Si bien se trata de conceptos íntimamente relacionados, existen pequeñas diferencias que son convenientes matizar:

- La «seguridad de la información» se refiere al conjunto de medidas preventivas que permiten almacenar y preservar la información de una empresa, una institución o un particular; por su parte, la «ciberseguridad» se centra solamente en la protección de los datos digitales y los sistemas interconectados que los procesan, almacenan o transmiten, de ataques maliciosos en el entorno cibernético.

- En segundo lugar, la «ciberseguridad» se basa en realizar ataques ofensivos contra las amenazas existentes, mientras que la «seguridad de la información» contempla aspectos defensivos para proteger los sistemas de información.

Puntualizado esto, pasamos a conocer cuáles son los principales ataques que se producen hoy en día.

2.2. Ciberamenazas: tipos y origen

2.2.1. Tipos de ciberamenazas

De acuerdo con el *Cisco Annual Cybersecurity Report*, los ataques cibernéticos más comunes son los siguientes:

Malware

Es un término genérico que abarca varias amenazas entre las que se incluyen: virus, gusanos, troyanos, *spyware* o *ransomwore*; entre otros.

Penetra la red una vez que el usuario hace clic en un enlace peligroso o en un archivo adjunto de correo electrónico que, consecuentemente, activa la instalación de un *software* malintencionado en el sistema informático.

Una vez dentro, puede hacer lo siguiente:

- Bloquear el acceso a los componentes críticos de la red
- Obtener información de los datos del disco duro
- Interrumpir — incluso inhabilitar — el equipo
- Instalar un *software* dañino adicional

Suplantación de identidad

También conocida como *phishing*; consiste, principalmente, en el envío masivo de correos electrónicos fraudulentos — con apariencia de proceder de una fuente fiable —, que incorporan un archivo o un *script* malicioso que permite a los atacantes acceder al dispositivo para controlarlo o extraer información sensible del usuario.

Se trata de una amenaza cada vez más frecuente ya que, también puede tener lugar a través de redes sociales y otras comunidades *online*, mensajes SMS (*smishing*) e, incluso, llamadas telefónicas (*vishing*).

Ataque de intermediario

Responde a las siglas MitM, por el nombre que recibe inglés: *Man-in-the-Middle*. Ocurren cuando el atacante intercepta una transacción entre dos partes y se inserta en ella, lo que le permite interrumpir el tráfico y así robar y manipular los datos. Normalmente, suele ocurrir cuando los usuarios están conectados a una red vulnerable, como son las de WiFi públicas.

Es muy difícil de detectar, pues la víctima piensa que está enviando la información a un destino legítimo.

Ataque de denegación de servicio

Los ataques DoS (*Denial of Service*) inundan sistemas, servidores y redes con tráficos con el objetivo de sobrecargar recursos y el ancho de la banda, y así impedir el procesamiento de las solicitudes legítimas. Si este se produce desde distintos puntos, estaríamos ante un ataque DDoS (*Distributed Denial of Service*).

Para ambos casos, la forma más común es a través de un conjunto de robots informáticos (*netbots*).

Inyección de SQL

Esta amenaza se basa en la inserción de un código malicioso en un servidor que utiliza un lenguaje de consulta estructurado y fuerza a este a que revele información. Normalmente, se produce a partir del envío de dicho código a un comentario o cuadro de búsqueda del sitio web no protegido.

Ataque de día cero

Considerado uno de los más peligrosos; se produce cuando una red es nueva y ha sido recientemente anunciada, previo a que un parche sea implementado, los atacantes aprovechan la vulnerabilidad revelada — desconocida para el usuario —, en esa pequeña ventana de tiempo para la que no existe ninguna medida preventiva.

Ataque de contraseña

Es el método más extendido para tratar de acceder a un sistema de información seguro. Para ello, los atacantes emplean varias técnicas que van desde el simple hecho de tratar de adivinar la contraseña al uso de ingeniería social.

No obstante, entre todas ellas, las dos principales son:

- Ataque de fuerza bruta: el atacante emplea un programa que prueba todas las combinaciones posibles de información.
- Ataque con diccionario: utiliza un listado de contraseñas comunes.

Secuencias de comandos en sitios cruzados

Los ataques XSS (del inglés, *Cross-Site Scripting)* se basan en la colocación de comandos maliciosos en sitios web y aplicaciones legítimas que, a su vez, instalan un *malware* en los navegadores web de los usuarios.

Rootkits

Se instalan dentro de un paquete de *software* legítimo para permanecer oculto en un equipo, y así obtener acceso y control remoto de la administración de este sin que el propietario se dé cuenta o haya dado su consentimiento.

Criptojacking

A raíz del aumento de inversiones en criptomonedas, cada vez es más común que los ciberdelincuentes intenten lucrarse a través de este tipo de ataque. Este se define como el uso no detectado de un dispositivo informático ajeno, no para acceder o extraer datos, sino para minar monedas digitales.

2.2.2. Origen de las amenazas

Se tiende a pensar que los ataques que se producen en el ciberespacio se originan de forma hostil por parte de piratas informáticos que, si bien es cierto resulta ser así en su gran mayoría, también se perpetran otros de manera no intencionada producidos por otros agentes.

A partir del estudio de *Ciberamenazas y Tendencias Edición 2020* elaborado por el Centro Criptológico Nacional de España (CCN-CERT), se presenta la siguiente relación entre los distintos agentes originarios de las amenazas y sus víctimas[1]:

ESTADOS Y GRUPOS PATROCINADOS POR ESTADOS

Víctimas	Amenazas		
Sector público	Ciberespionaje	Manipulación de información	Acciones híbridas
Infraestructuras críticas	Ciberespionaje	Interrupción de servicios	
Empresas	Ciberespionaje	Manipulación de sistemas	
Ciudadanos	Influencia	Ciberespionaje	

Elaboración propia a partir de CCN-CERT

[1] Los colores indican el índice de peligrosidad: alto (rojo), naranja (medio) y amarillos (bajo).

CIBERDELINCUENTES

Víctimas	Amenazas			
Sector público	Interrupción de servicios		Manipulación de sistemas	Robo de información
Infraestructuras críticas	Interrupción de servicios		Manipulación de sistemas	
Empresas	Robo de información	Manipulación de información	Interrupción de servicios	Manipulación de sistemas
Ciudadanos	Manipulación de sistemas	Interrupción de servicios	Manipulación de información	Robo de información

Elaboración propia a partir de CCN-CERT

TERRORISTAS

Víctimas	Amenazas
Sector público	Sabotaje
Infraestructuras críticas	Sabotaje

Elaboración propia a partir de CCN-CERT

HACKTIVISTAS

Víctimas	Amenazas		
Sector público	Interrupción de servicios	Manipulación de información	
Infraestructuras críticas	Interrupción de servicios	Manipulación de información	
Empresas	Interrupción de servicios	Robo de información	Manipulación de información

Elaboración propia a partir de CCN-CERT

INSIDER[2]

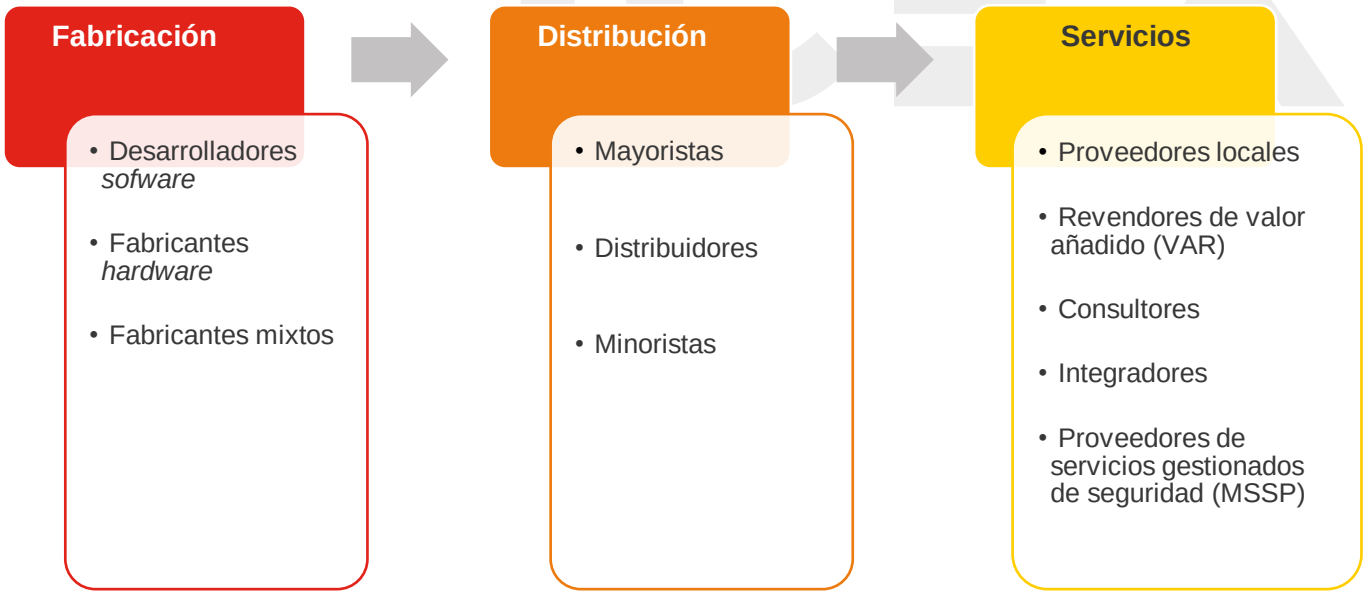
Víctimas	Amenazas	
Sector público	Robo de información	Interrupción de servicios
Infraestructuras críticas	Robo de información	Interrupción de servicios
Empresas	Robo de información	Interrupción de servicios

Elaboración propia a partir de CCN-CERT

2.3. Cadena de valor y canales de distribución

Según el Instituto Nacional de Ciberseguridad de España (INCIBE), la cadena valor del sector de objeto de estudio se compone de tres grandes actividades que pueden observarse en el gráfico inferior:

CADENA DE VALOR DEL SECTOR DE LA CIBERSEGURIDAD



Fuente: elaboración propia a partir de INCIBE

La **fabricación** incluye a los diferentes agentes que se encargan de la producción de las soluciones de ciberseguridad:

[2] Se refiere a toda persona que, por la naturaleza de su trabajo, tiene acceso a los sistemas y archivos internos.

- Desarrolladores de *software*: suministran soluciones y aplicaciones no físicas que garantizan la seguridad en la red y contribuyen a gestionar y controlar el acceso web de los usuarios.
- Fabricantes de *hardware*: aportan soluciones y herramientas físicas, así como sistemas y aplicaciones que garantizan la seguridad en las redes corporativas.
- Fabricantes mixtos: proporcionan tanto productos *hardware* como *software*.

La siguiente fase de la cadena — **distribución** — se compone de las empresas que actúan como nexo entre las actividades de fabricación y prestación del servicio. En este, se incluyen:

- Mayoristas: se dedican a comprar y vender los productos a consultoras, integradores y proveedores de servicios de seguridad.
- Distribuidores: venden tanto a empresas del sector como a los propios clientes finales.
- Minoristas: a menudo, se trata de puntos de venta físicos que se dirigen principalmente a pequeñas y medianas empresas, y también a los particulares.

Para finalizar, el eslabón de los **servicios** engloba los siguientes elementos:

- Proveedores locales: proporcionan servicios personalizados a través del desarrollo de productos propios.
- Revendedores de valor añadido (VAR): ofrecen un servicio completo a partir de agregar valor añadido a los productos *software* y *hardware* fabricados por otros.
- Consultoras: pueden ser de negocio, que asesoran sobre asuntos legales y organizativos de la ciberseguridad; o tecnológicas, que dan respuesta y ofrecen soporte a situaciones relativas a la tecnología.
- Integradores: crean soluciones complejas que se adaptan a las necesidades de los usuarios.
- Proveedores de servicios gestionados de seguridad (MSSP): desde un enfoque integral y multidisciplinar de la seguridad corporativa, proporcionan servicios externalizados al cliente.

2.4. Soluciones

Dentro del rubro objeto de estudio, se distinguen tres principales áreas de actuación:

1. Soluciones de prevención: incluye tecnologías que tratan de evitar un ciberataque.
2. Soluciones de mitigación: permiten detectar el impacto del ataque en proceso y limitar el daño producido.
3. Soluciones de control: se encargan de la legislación y administración de las diferentes alternativas de ciberseguridad.

En las siguientes tablas se muestran las distintas soluciones incluidas en la clasificación anterior, por tipología y categoría de productos:

TABLA 1: SOLUCIONES DE PREVENCIÓN

Solución	Producto
Anti-*malware*	• Anti-virus • Anti-*adware* • Anti-*spyware* • *Unified Threat Management* (UTM)
Anti-fraude	• Anti-*phising* • Anti-*spam* • Herramientas de filtrado de navegación • UTM
Prevención de fuga de información	• Control de contenidos confidenciales • *Information Life Cycle Management* (ILCM) • Control de dispositivos externos de almacenamiento • Herramientas de cifrado • Cifrado de discos duros y soportes de almacenamiento
Protección de las comunicaciones	• Cortafuegos • *Virtual Private Network* (VPN) • *Routers* seguros • UTM • *Intrusion Prevention System* (IPS) • *Intrusion Detention System* (IDS) • Cifrado de las comunicaciones • Filtro de contenidos • Herramientas de control P2P • Gestión y control de ancho de banda • Herramientas de monitorización y *reporting* • Seguridad en el correo • Seguridad en la web
Seguridad en dispositivos móviles	• Seguridad para dispositivos móviles • Seguridad para redes inalámbricas • Seguridad para BYOD

Fuente: elaboración propia a partir de CCN-CERT

TABLA 2: SOLUCIONES DE MITIGACIÓN

Solución	Producto
Contingencia y continuidad	• Gestión de planes de contingencia y continuidad • Herramientas de recuperación de sistemas • Copias de seguridad • Infraestructuras de respaldo • Seguridad en virtualización • Herramientas de seguridad en la nube • Ciberseguros
Inteligencia de seguridad	• *Security Event Management* (SEM) • *Security Information Management* (SIM) • *Security Information and Event Management* (SIEM) • Soluciones *Big Data*

	• Herramientas de monitorización y *reporting*

Fuente: elaboración propia a partir de CCN-CERT

TABLA 3: SOLUCIONES DE CONTROL

Solución	Producto
Auditoría técnica	• Análisis de *logs* y puertos • Análisis de vulnerabilidades • Auditoría de contraseñas • Auditoría de sistemas y ficheros • Auditoría de red • Herramientas de recuperación de datos • Herramientas de testeo de *software* y aplicaciones web
Certificación normativa	• Sistemas de Gestión de la Seguridad de la Información (SGSI) • Análisis de riesgos • Planes y políticas de seguridad • Normativa de seguridad
Cumplimiento legal	• Herramientas de cumplimiento legal • Borrado seguro • Destrucción documental
Control de acceso y autenticación	• *Network Access Control* (NAC) • Gestión de identidad y autenticación • Herramientas de autenticación o validación única • Certificados digitales • Firma electrónica • Tarjetas inteligentes y dispositivos biométricos • *Brokers* de acceso *cloud*

Fuente: elaboración propia a partir de CCN-CERT

2.5. Posición arancelaria

Debido a su naturaleza intangible, los servicios de ciberseguridad no se encuentran clasificados en la codificación arancelaria utilizada en los países del Mercosur, motivo por el cual resulta complicado su contabilización.

3. Oferta – Análisis de competidores

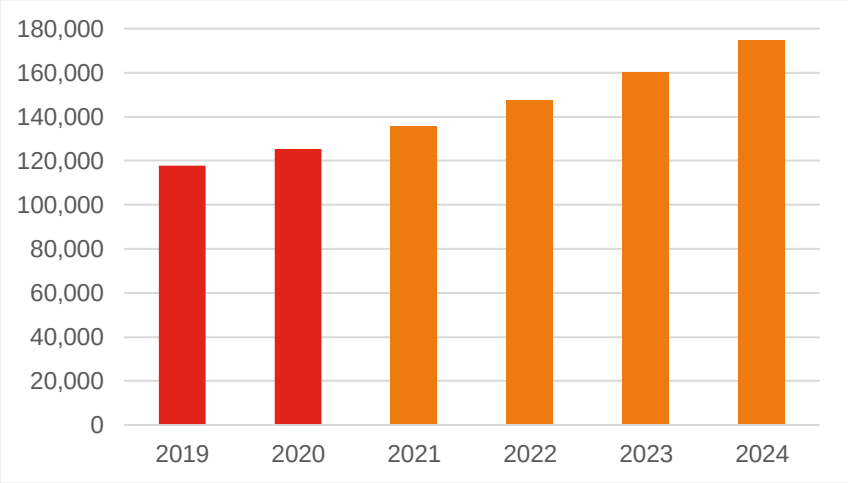
3.1. Proyecciones del mercado mundial

Como consecuencia de la pandemia, millones de trabajadores comenzaron a trabajar en la modalidad de *home office* con equipos desprotegidos, lo que provocó que la magnitud y la frecuencia de los ciberataques aumentase, y esto se vea reflejado en el impacto económico que están alcanzando tal y como se detalla en este apartado. Por esta razón, la ciberseguridad ha pasado a ser una prioridad en la gestión de los riesgos que sufren, no solo los usuarios particulares, sino, especialmente, las empresas, gobiernos e infraestructuras clave.

La relevancia de esta amenaza queda patente en el *Informe de Riesgos 2020* que cada año elabora el Foro Económico Mundial, con la inclusión de dos riesgos relacionados con la ciberseguridad en la lista de los cinco principales peligros para el mundo.

De acuerdo con la *International Data Corporation* (IDC), la cifra de mercado del sector alcanzó los 125.200 millones de dólares el año pasado, lo que supuso un 6 % más con respecto a 2019. Sin embargo, debido a lo expuesto previamente, se estima que esta cifra alcance los 174.400 millones en 2024, con una tasa de crecimiento compuesta anual del 8,1 %.

EL MERCADO MUNDIAL DE LA CIBERSEGURIDAD
Tamaño del mercado y previsiones (millones de USD)

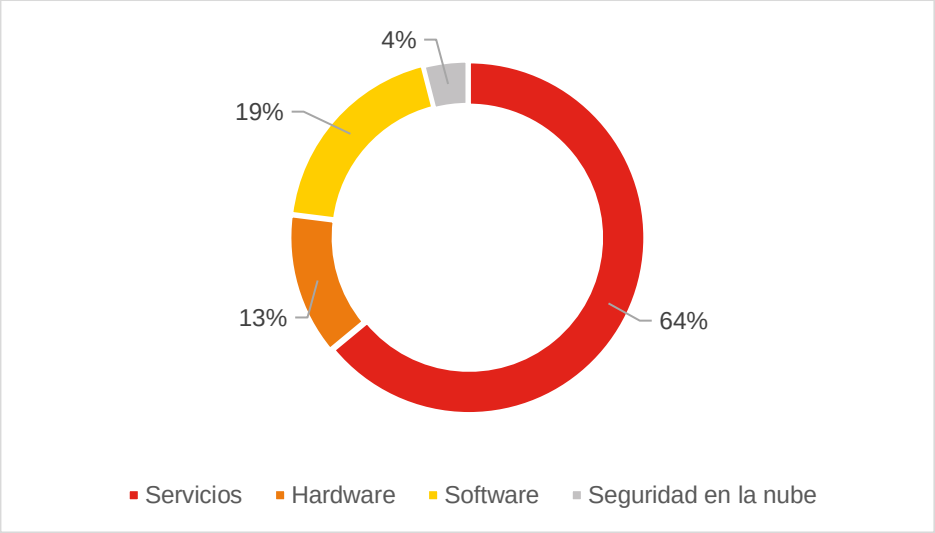


Fuente: elaboración propia a partir de IDC

Por su parte, la misma fuente también revela que la inversión realizada el año pasado, se distribuyó de la siguiente manera:

EL MERCADO MUNDIAL DE LA CIBERSEGURIDAD

Tamaño del mercado por tipo de prestación (%)

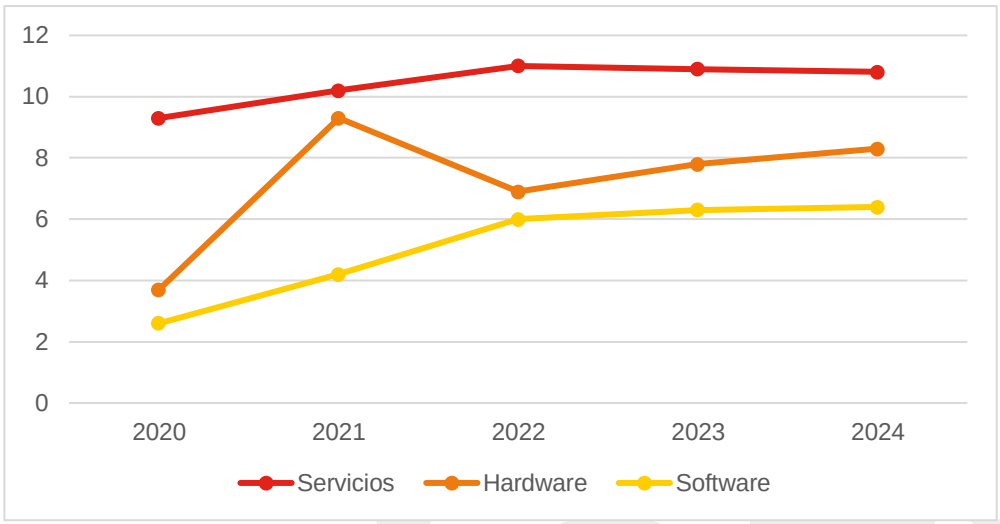


Fuente: elaboración propia a partir de IDC

Asimismo, se proyecta que el crecimiento interanual del gasto en *software*, *hardware* y servicios de ciberseguridad evolucionen de acuerdo con el siguiente gráfico:

EL MERCADO MUNDIAL DE LA CIBERSEGURIDAD

Proyecciones de crecimiento interanual por tipo de prestación (%)



Fuente: elaboración propia a partir de IDC

Si bien se aprecia como la pandemia ha afectado positivamente a las inversiones a realizar en el sector, cabe destacar el gasto estimado para las soluciones *hardware* en 2021, con un incremento anual próximo al 10 %.

Por último, la empresa *Cybersecurity Ventures*, líder en investigación sobre economía cibernética a nivel mundial, publicó una serie de proyecciones del sector para este año que conviene incluir en este estudio; estas son:

1. **Se prevé que los daños financieros mundiales causados por el crimen cibernético lleguen a 6 billones de dólares en 2021.**

Para hacerse una idea de lo que esto supone, si se consideraran los daños derivados del cibercrimen como si fuese la economía de un país, estaríamos ante la tercera más grande del mundo, solamente por detrás de Estados Unidos y China.

En 2015, dichos costes alcanzaron los 3 billones de dólares y las perspectivas indican que aumentarán un 15 % cada año hasta los 10,5 billones en 2025.

2. **Los ataques de *ransomware* supondrán un coste de 20.000 millones de dólares en 2021.**

Este tipo de *malware* — infecta los ordenadores y demás dispositivos tecnológicos restringiendo el acceso a los datos archivados y, a menudo, implica la destrucción de los mismos — se ha convertido en una de las formas de atacar más frecuentes por parte de los cibercriminales.

Según los datos recabados en el informe, los daños mundiales derivados por *ransomware* se prevé que aumenten un 57 % más que las cifras registradas en 2015. De hecho, se estima que cada 11 segundos, se produzca un ataque de este tipo en el mundo.

3. **La ciberseguridad creará 3,5 millones de puestos de trabajo en 2021.**

Por cada vacante en el sector de las tecnologías de la información se precisa otro trabajador que se dedique a la protección y defensa de los dispositivos, las aplicaciones y los datos generados y archivados en ellos.

Desde 2011, la tasa de desempleo en el rubro de la ciberseguridad está en 0 %.

4. **En 2021, más del 70 % de las transacciones con criptomonedas están relacionadas con actividades ilegales.**

Consecuentemente al auge de las inversiones en divisas virtuales, el criptodelito es un segmento emergente dentro de los ataques que se producen en el ciberespacio, cuya predicción para este año es que el 70 % de las transacciones anuales de criptomonedas — 50 % de *bitcoin* y el 20 % del resto — se corresponderán con actividades ilícitas.

3.2. El mercado latinoamericano

Se tiende a pensar que los ciberataques ocurren en menor medida en América Latina debido al menor grado de penetración en internet en comparación con el resto de países del mundo. Sin embargo, ocurre todo lo contrario, pues cada vez es más común el uso de nuevas tecnologías en esa parte del continente.

De acuerdo con el estudio *Internet World Stats*, elaborado por la Comisión Económica para América Latina y el Caribe (CEPAL), la región pasó de tener una penetración en internet de 43,4 % en 2015 a 71,5 % el año pasado; superando incluso el promedio mundial actual: 62 %.

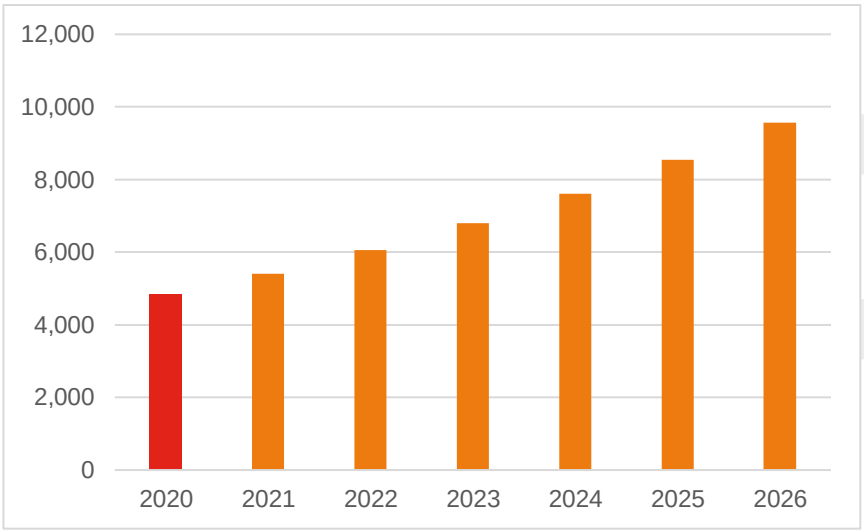
En consecuencia, el número de ciberataques ha ido en aumento en los últimos años y según el mapa en tiempo real de amenazas de la firma Kaspersky, en 2020, los países latinoamericanos ya se encontraban dentro del primer 25 % de los países más atacados del planeta, destacando el caso particular de Brasil: tercero en ataques registrados.

Por ello, y en especial debido a las vulnerabilidades derivadas del brote de la pandemia, la seguridad cibernética se ha convertido en una necesidad absoluta para las empresas y las organizaciones radicadas en alguno de estos países.

El año pasado, según datos publicados en el informe *Latin America Cyber Security Market - Growth, Trends, Covid-19 Impact, And Forecasts 2021-2026* elaborado por *Mordor Intelligence*, el valor del mercado de la ciberseguridad en América Latina fue de 4.840 millones de dólares y se proyecta que en 2026 alcance los 9.570 millones, con una tasa de crecimiento compuesta anual superior a la mundial: 10,8 %.

EL MERCADO LATINOAMERICANO DE LA CIBERSEGURIDAD

Tamaño del mercado y previsiones (millones de USD)



Fuente: elaboración propia a partir de Mordor Intelligence

Sin embargo, este mismo estudio revela un factor preocupante que limita el crecimiento del mercado en la región: la falta de profesionales especialistas.

Este hecho lo confirma también el reporte *Ciberseguridad Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe 2020* publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), según el cual dos tercios de los países presentan pocas o nulas mejoras respecto a la educación y capacitación de habilidades en seguridad cibernética, y la oferta de formación especializada es inexistente.

3.3. El mercado argentino

3.3.1. Situación actual del sector

A pesar del reciente crecimiento del mercado local, la implementación de la seguridad cibernética en Argentina todavía se encuentra en su etapa inicial de madurez; un par de años por detrás de los mercados referentes del sector, como puede ser el caso de Estados Unidos o Reino Unido. Además, este proceso de crecimiento se ve obstaculizado por las constantes fluctuaciones del tipo de cambio y la devaluación del peso.

No obstante, la sociedad argentina — especialmente el colectivo empresarial — es cada más consciente de los problemas ocasionados por el cibercrimen. En parte, esto se debe al compromiso cibernético que se mencionaba en el apartado anterior. Argentina se encuentra dentro de un reducido grupo de países en Latinoamérica que cuentan con una estrategia nacional de ciberseguridad y que han desarrollado una oferta educativa que les permite contar con una población bien conocedora de este tipo de tecnología.

En los últimos años, se han tomado numerosas medidas para implementar políticas y realizar cambios administrativos y regulatorios que han afectado de manera positiva al rubro:

Política y administración

Los primeros pasos se dan en 2011 con la aprobación del Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), desarrollado para fijar un marco regulatorio que permitiese definir y proteger la infraestructura estratégica y crítica de los sectores público y privado, así como de las organizaciones interjurisdiccionales.

Años más tarde, en 2017, se crea el Comité de Ciberseguridad, órgano dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros, con el objetivo de desarrollar una estrategia nacional de seguridad cibernética.

Otro de los cambios administrativos que tuvieron lugar durante ese año fue la creación de la Subsecretaría de Ciberdefensa en el Ministerio de Defensa y de la Dirección de Cibercrimen en el Ministerio de Seguridad. También, se establecieron unidades especializadas en cibercrimen tanto a nivel nacional como en la jurisdicción de la Ciudad Autónoma de Buenos Aires.

Por su parte, la Estrategia Nacional de Ciberseguridad no se aprobó hasta el 2019, cuya Unidad Ejecutora actúa bajo las directrices de la Secretaría de Modernización de la Nación.

Asimismo, en ese año, el BID brindó su apoyo al gobierno argentino a través de la aprobación de un préstamo para la implementación de políticas relativas a la seguridad de los datos personales y la buena praxis en el uso de las TIC, con acciones puntuales hacia el fortalecimiento de la ciberseguridad.

Educación

Respecto a las medidas tomadas para formar a la población argentina en el rubro, son varias las universidades, tanto públicas como privadas, que ofrecen una educación en seguridad cibernética

Por otro parte, el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BA-CSIRT) también da la oportunidad mediante charlas de sensibilización sobre seguridad cibernética y el uso de las TIC.

3.3.2. Datos sobre ciberataques en Argentina

De acuerdo con el *Global Cybersecurity Index*, que elabora anualmente la International Telecommunication Union (ITU), Argentina se sitúa en la posición 91 del ranking mundial que mide la seguridad cibernética de 194 naciones.

TABLA 4: RANKING MUNDIAL DE LA CIBERSEGURIDAD

Posición ranking mundial	País	Puntuación
1	Estados Unidos	100
2	Reino Unido	99,54
	Arabia Saudí	99,54
3	Estonia	99,48
4	Corea del Sur	98,52
	Singapur	98,52
	España	98,52
5	Rusia	98,06
	Malasia	98,06
6	Lituania	97,93
7	Japón	97,82
8	Canadá	97,67
9	Francia	97,60
10	India	97,50
91	**Argentina**	**50,12**[3]

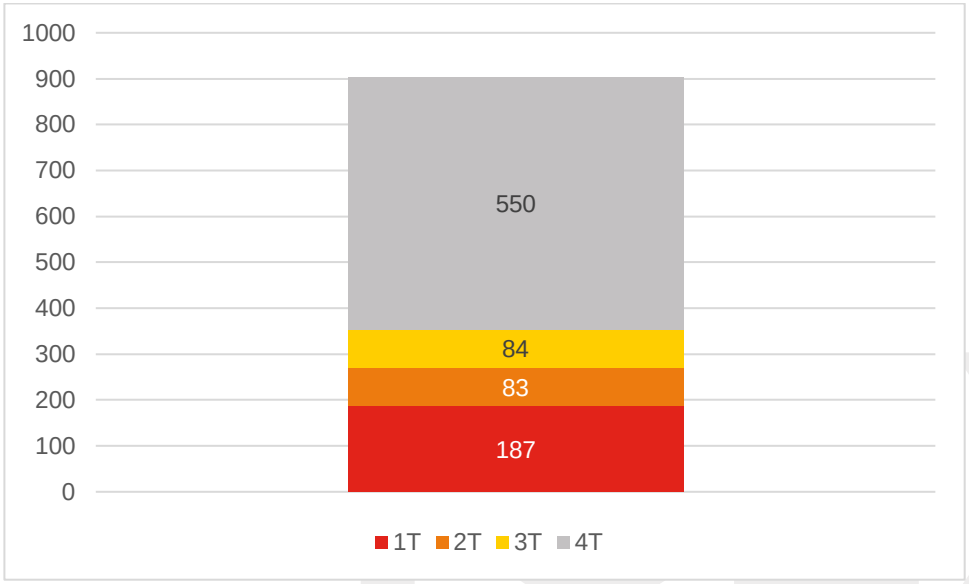
Fuente: elaboración propia a partir de ITU

[3] Para conocer el desglose de la puntuación obtenida por Argentina, ver Anexo I.

Durante el año pasado, el cibercrimen en el país se cifró en 904 millones de ataques, solamente superado por Brasil y México en la región latinoamericana. De estos, la mayoría se produjo en el último trimestre del año, tal y como se puede apreciar en el siguiente gráfico:

CIBERATAQUES EN ARGENTINA EN 2020

Número de ciberataques por trimestres (millones de uds.)



Fuente: elaboración propia a partir de Fortinet

Un año más, las campañas de *phishing* fueron el principal vector de ataque: 1,65 millones de amenazas — 4.509 al día —, según las cifras recabadas por una de las principales empresas de seguridad informática del mundo: Kaspersky.

TABLA 5: RANKING MUNDIAL DE ATAQUES *PHISHING* EN 2020

Posición ranking mundial	País
1	Brasil
2	Venezuela
3	Portugal
4	Australia
5	España
26	**Argentina**

Fuente: elaboración propia a partir de Kaspersky

Asimismo, también conviene destacar el crecimiento interanual de las diferentes modalidades de *malware*: 26 %. De acuerdo con la misma fuente anterior, se cometieron cerca de 25 millones de ataques de este tipo, que afectaron a 160.000 usuarios.

TABLA 6: RANKING MUNDIAL DE ATAQUES *MALWARE* EN 2020

Posición ranking mundial	País
1	Estados Unidos
2	India
3	Rusia
4	Alemania
5	Brasil
59	**Argentina**

Fuente: elaboración propia a partir de Kaspersky

Por último, para conocer la tipología de las amenazas registradas — virus, *botnets* y *exploits* — en el país durante el último trimestre del año pasado y el primero de 2021, ver Anexo II y III.

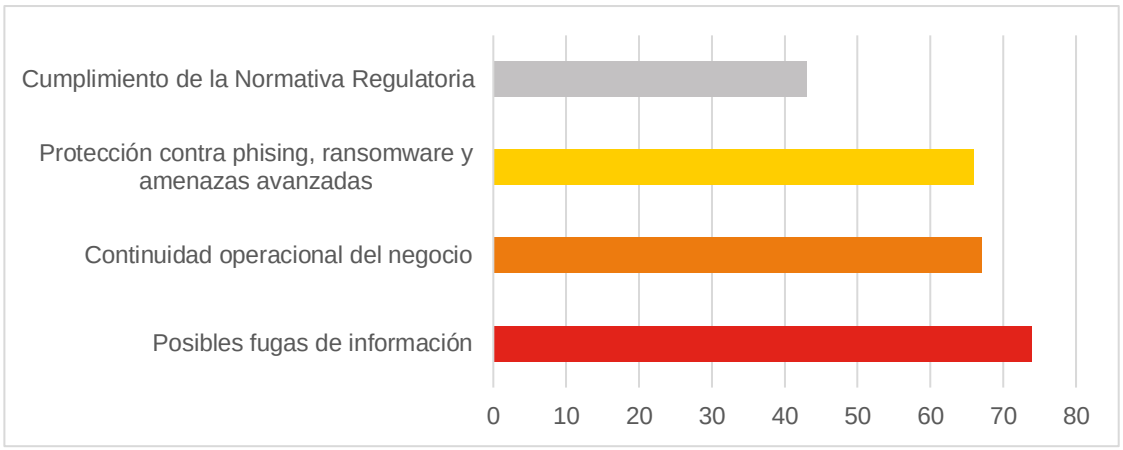
3.3.3. Ciberseguridad en las empresas argentinas

A principios de año, Microsoft Argentina publicó su informe *Ciberseguridad en las Empresas de Argentina* en el que participaron 200 compañías líderes del país, el cual ofrece una serie de observaciones que conviene incluir en este estudio.

Primeramente, la principal preocupación respecto a la seguridad cibernética de sus negocios son las posibles fugas de información. El resto de las respuestas más repetidas a esta pregunta — multirrespuesta — fueron las siguientes:

PRINCIPALES PREOCUPACIONES DE LAS EMPRESAS ARGENTINAS

Respuesta multirrespuesta expresada en %

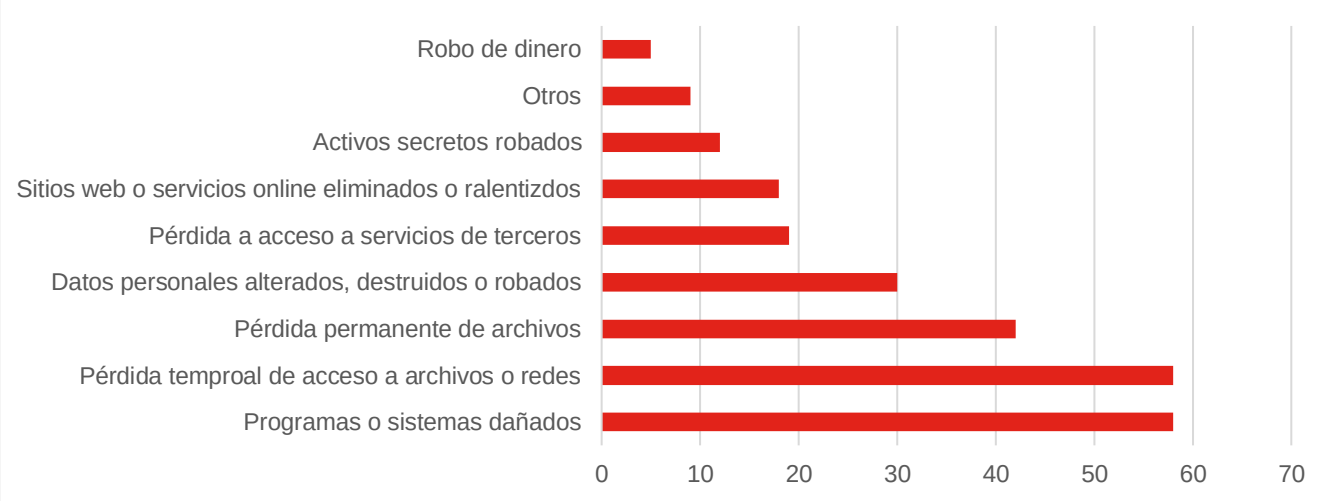


Fuente: elaboración propia a partir de Microsoft Argentina

En relación con los ataques sufridos durante el 2020, el 65 % de las firmas participantes aseguran haber sufrido al menos uno. Por su parte, las consecuencias más comunes han sido tanto la pérdida temporal de acceso a archivos o redes como el daño a programas o sistemas.

PRINCIPALES CONSECUENCIAS DE LOS CIBERATAQUES

Respuesta multirrespuesta expresada en %

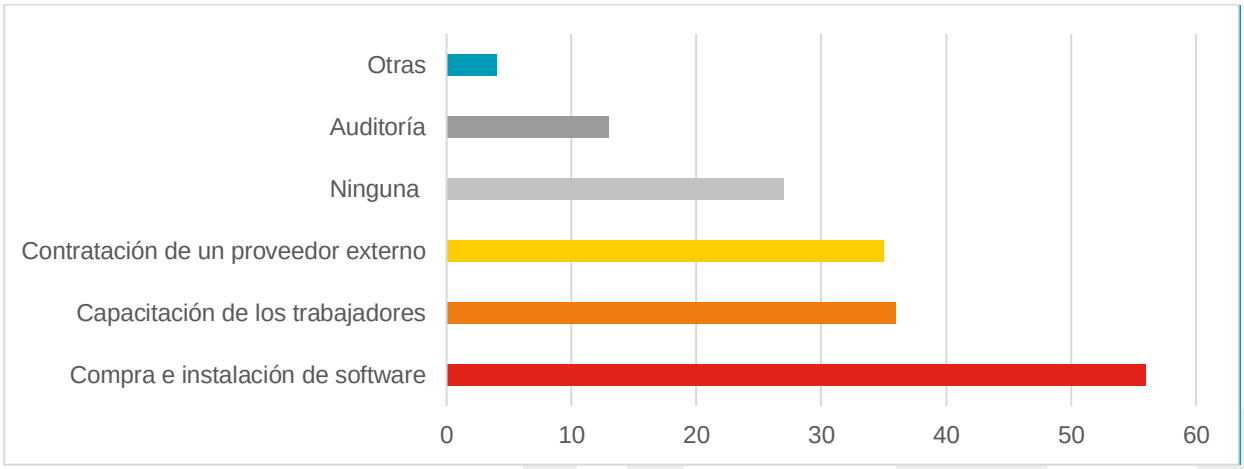


Fuente: elaboración propia a partir de Microsoft Argentina

Con el fin de evitar que estos continúen repitiéndose, la medida que mayoritariamente han tomado las empresas encuestadas ha sido la compra e instalación de un *software* que permita mejorar su seguridad actual. Igualmente, también ha habido otras adicionales:

PRINCIPALES MEDIDAS FRENTE A LOS CIBERATAQUES

Respuesta multirrespuesta expresada en %



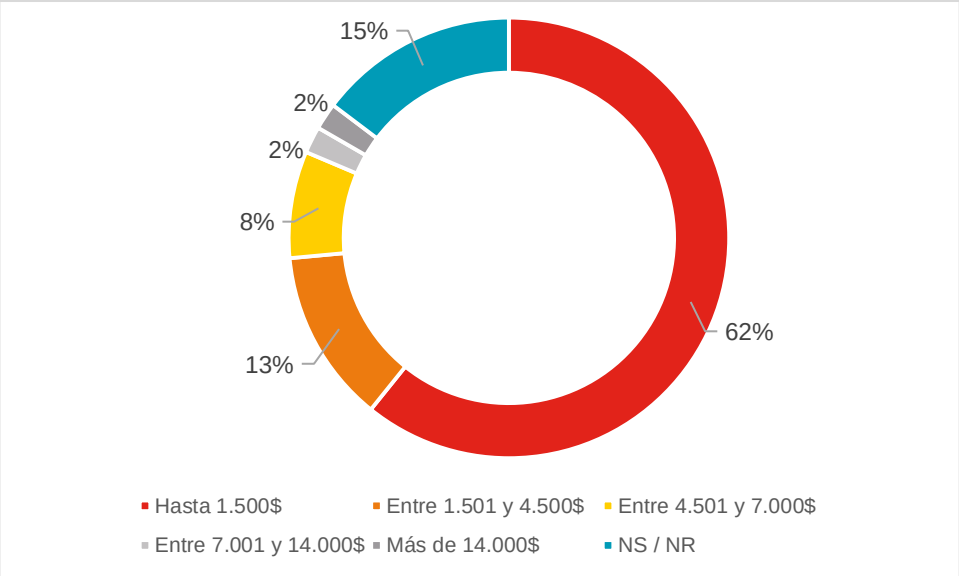
Fuente: elaboración propia a partir de Microsoft Argentina

Pese a ello, el 24 % de las empresas considera que es probable que a lo largo del 2021 vuelvan a sufrir un nuevo ataque cibernético. Este porcentaje aumenta entre aquellas que fueron víctimas en algún momento del año pasado: 4 de cada 10 considera que nuevamente se verán afectadas por el cibercrimen.

Por último, con relación al gasto[4] realizado en ciberseguridad, el 62 % no invirtió más de 1.500 dólares en los últimos 12 meses.

[4] Incluye *software*, *hardware*, sueldos, capacitaciones, *outsourcing*, etc., pero deja fuera los gastos asociados a reparar daños causados por un ciberataque

GASTO REALIZADO EN CIBERSEGURIDAD



Fuente: elaboración propia a partir de Microsoft Argentina

Igualmente, el 43 % de las compañías consideran que la inversión es suficiente, pero que se debería adquirir otro tipo de tecnologías. Así lo comparten las empresas que sufrieron al menos un ataque en 2020, pues en su caso, la repuesta es la misma para el 63 % de ellas.

3.3.4. Análisis cualitativo de la ciberseguridad en Argentina

El informe *Ciberseguridad Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe 2020* previamente mencionado en el apartado 3.2, incluye una ficha específica para cada país basada en los datos analizados de 52 indicadores del modelo de madurez de la capacidad de seguridad cibernética desarrollado por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford (GCSCC), y divididos en cinco dimensiones.

A continuación, se recopilan los datos de Argentina: en amarillo se representa el estado de capacitación en 2016 y en naranja la mejora de los indicadores hasta 2020.

POLÍTICA Y ESTRATEGIA DE SEGURIDAD CIBERNÉTICA

	1	2	3	4	5
Estrategia nacional de ciberseguridad					
Desarrollo de la Estrategia					
Organización					
Contenido					
Estrategia nacional de ciberseguridad					
Identificación de incidentes					
Organización					
Coordinación					
Modo de operación					
Protección de la Infraestructura Crítica					
Identificación					
Organización					
Gestión de riesgos y respuesta					
Manejo de crisis					
Manejo de crisis					
Defensa cibernética					
Estrategia					
Organización					
Coordinación					
Redundancia de comunicaciones					
Redundancia de comunicaciones					

Fuente: elaboración propia a partir del BID y la OEA

CULTURA CIBERNÉTICA Y SOCIEDAD

	1	2	3	4	5
Mentalidad de seguridad cibernética					
Desarrollo de la Estrategia					
Organización					
Contenido					
Confianza y seguridad en internet					
Confianza y seguridad del usuario en internet					
Confianza del usuario en los servicios electrónicos del Gobierno					
Confianza del usuario en los servicios de comercio electrónico					
Comprensión del usuario de la protección de la información en línea					
Comprensión del usuario de la protección de información personal en línea					
Mecanismos de denuncia					
Mecanismos de denuncia					
Medios y redes sociales					
Medios y redes sociales					

Fuente: elaboración propia a partir del BID y la OEA

FORMACIÓN, CAPACITACIÓN Y HABILIDADES DE SEGURIDAD CIBERNÉTICA

	1	2	3	4	5
Sensibilización					
Programas de sensibilización					
Sensibilización ejecutiva					
Marco para la formación					
Provisión					
Administración					
Marco para la capacitación profesional					
Provisión					
Apropiación					

Fuente: elaboración propia a partir del BID y la OEA

MARCOS LEGALES Y REGULATORIOS

	1	2	3	4	5
Macros legales					
Marcos legislativos para la seguridad de las TIC					
Privacidad, libertad de expresión y otros derechos humanos en línea					
Legislación sobre protección de datos					
Protección infantil en línea					
Legislación de protección al consumidor					
Legislación de propiedad intelectual					
Legislación sustantiva contra el delito cibernético					
Legislación procesal contra el delito cibernético					
Sistema de justicia penal					
Fuerzas del Orden					
Enjuiciamiento					
Tribunales					
Marcos de cooperación formales e informales para combatir el delito cibernético					
Cooperación formal					
Cooperación informal					

Fuente: elaboración propia a partir del BID y la OEA

ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS

	1	2	3	4	5
Cumplimiento de los estándares					
Estándares de seguridad de las TIC					
Estándares en adquisiciones					
Estándares en el desarrollo de *software*					
Resiliencia de la infraestructura de internet					
Resiliencia de la infraestructura de internet					
Calidad del *software*					
Calidad del software					

Controles técnicos de seguridad					
Controles técnicos de seguridad					
Controles criptográficos					
Controles criptográficos					
Mercado de seguridad cibernética					
Tecnologías de seguridad cibernética					
Seguro cibernético					
Divulgación responsable					
Divulgación responsable					

Fuente: elaboración propia a partir del BID y la OEA

3.4. Competidores

A continuación, se mencionan a las principales empresas competidoras que actúan en el mercado argentino; se incluye el enlace directo a sus sitios web para poder ampliar información de cada una.

3.4.1. Empresas internacionales

Fortinet, una de las firmas líderes a nivel mundial (ver Anexo IV) de las soluciones en ciberseguridad, ha consolidado su liderazgo en Argentina, tras alcanzar un 43 % de la cuota de mercado en 2020.

El resto de las principales empresas a nivel internacional que también están presentes en el país son las siguientes:

IBM

Symantec

Cisco	McAfee

3.4.2. Empresas argentinas

Por su parte, la competencia nacional está muy fragmentada. Entre las más destacadas se encuentran las siguientes:

Amalgama	Simplex Software	Neginet	Vates
DinoCloud	IncluIT	Zarego	
Julasoft	Wolox	FlyDevs	Grupo Datco

Cloud Legion	Core Security	Onapsis

4. Demanda

4.1. Principales clientes del sector

De acuerdo con el informe de *Tendencias en el Mercado de la Ciberseguridad* elaborado por el INCIBE, los principales demandantes de los servicios de seguridad cibernética se clasifican en los siguientes cuatro grandes grupos:

PRINCIPALES CLIENTES DEL SECTOR DE LA CIBERSEGURIDAD

Fuente: elaboración propia a partir de INCIBE

Administración Pública

El sector público requiere de soluciones de seguridad integral — reactiva, proactiva y de gestión — que permitan proteger a los diferentes organismos administrativos locales, regionales y nacionales.

Esta necesidad proviene, principalmente, de las amenazas producidas por el espionaje cibernético y la sustracción de información sensible que, habitualmente, termina vendiéndose o publicándose en internet.

Grandes empresas y operadores críticos

Además de demandar soluciones integrales, este grupo es destinatario de soluciones industriales con una alta especialización en el sector de actividad o la tecnología con la que se desarrolla esta.

Por su parte, son susceptibles de ataques de ciberespionaje industrial, de interrupción y control de sistemas, así como también de la sustracción y venta de información confidencial.

Pymes y autónomos

Esta tipología de clientes precisa de herramientas estándar desarrolladas por proveedores de ciberseguridad que adaptan sus servicios a pequeñas empresas o usuarios individuales.

Las principales amenazas que sufren se basan en el uso — a veces, incluso la reventa — de información privada que proporcionan los clientes a estas organizaciones privadas.

Particulares

Las soluciones de ciberseguridad para el usuario individual son herramientas genéricas enfocadas a cualquier destinatario y cuya utilización deriva de un uso habitual de internet.

Igual que en el caso anterior, las principales amenazas surgen del uso — y a veces, reventa — de información privada de la ciudadanía; cada vez son mayores debido al crecimiento del comercio electrónico.

4.2. Sectores clave

Con el objetivo de cuantificar la demanda de productos y servicios de ciberseguridad, primeramente, se tendrán en cuenta los sectores claves con mayor probabilidad de ser víctimas de un ciberataque.

En el caso del mercado a nivel mundial, estos coinciden con los rubros más expuestos y, por ende, los que se ven necesitados de adoptar mayores soluciones de seguridad cibernética.

De acuerdo con el *X-Force Threat Intelligence 2021* publicado a principios de año por IBM, los sectores de actividad más damnificados son los siguientes:

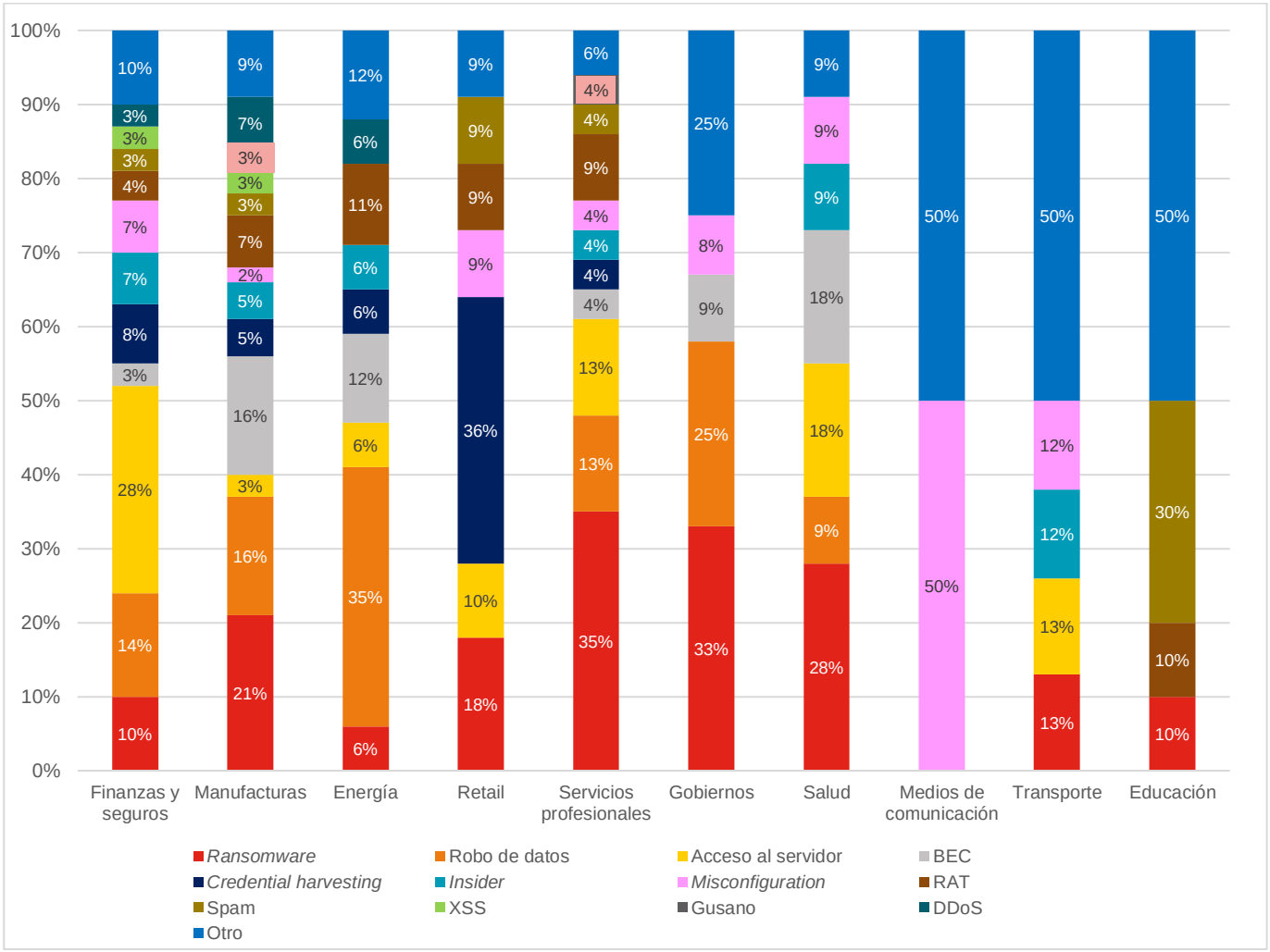
TABLA 7: SECTORES DE ACTIVIDAD MÁS AFECTADOS POR EL CIBERCRIMEN
Ranking expresado en %

Posición ranking mundial	Sector	% total de ataques	
		2019	2020
1	Finanzas y seguros	17%	23%
2	Manufacturas	8%	17,7%
3	Energía	6%	11,1%
4	*Retail*	16%	10,2%
5	Servicios profesionales	10%	8,7%
6	Gobiernos	8%	7,9%
7	Salud	6%	6,6%
8	Medios de comunicación	10%	5,7%
9	Transporte	10%	5,1%
10	Educación	8%	4%

Fuente: elaboración propia a partir de IBM

En cuanto a la tipología de ataques más comunes, según la actividad, se puede apreciar en el siguiente gráfico que estos son muy dispares. Por ejemplo, en el sector de las «Finanzas y seguros», casi un 30 % de estos se produjeron a través del acceso al servidor, mientras que en los rubros de la «Salud» y los «Servicios profesionales» los principales daños fueron causados por *ransomware*.

TIPOLOGÍA DE CIBERATAQUES POR SECTOR DE ACTIVIDAD



Fuente: elaboración propia a partir de IBM

4.2.1. El sector más afectado en Argentina

De acuerdo con la plataforma *Fortinet Threat Intelligence Insider Latin America*, gran parte de los intentos de ciberataque ocurridos en Argentina durante el año pasado siguen la misma tendencia observada a nivel mundial: estar diseñados para entrar en redes bancarias, obtener información financiera y robar dinero.

Por este motivo, el sector más damnificado ha vuelto a ser el de las finanzas; fundamentalmente, el bancario. El 27 % de los ataques fueron dirigidos a entidades financieras y a sus clientes; principalmente, a través de Twitter e Instagram.

En este sentido, las dos principales amenazas dirigidas a dicho sector fueron las siguientes:

- DoublePulsar: se trata de un ataque *backdoor*[5] utilizado en intrusiones a los bancos del país desde 2018.
- Emotet: es un *botnet* que permite al atacante emitir comandos para realizar diferentes operaciones tales como descargas de *malware* y *ransomware*.

Por otro lado, la elevada cifra de delitos registrada también estuvo muy ligada a las diversas campañas de *phishing* que apuntaban al robo de claves para el acceso al *home banking*. Desde 2018, los ataques a la banca electrónica vienen en aumento y se estima que, incluso, puedan seguir haciéndolo en los próximos años.

Con relación a esto, durante el primer semestre de 2020, se produjeron un número significativo de estafas mediante campañas por correo electrónico relacionadas a la COVID-19. Sin embargo, la mayor preocupación entre las entidades financieras derivó del nuevo *modus operandi* de los ciberdelicuentes: engañar a los usuarios a través de las redes sociales, tal y como se menciona anteriormente. Como las sucursales se encontraban cerradas, los clientes se dirigían confiados a las cuentas oficiales de los bancos a través de canales públicos, compartiendo así la información relativa a sus solicitudes y reclamos, a la vista de los *hackers*.

Este hecho provocó que algunas entidades optaran por suspender momentáneamente su actividad en dichas redes sociales con el objetivo de proteger a su clientela; esto fue el caso del Banco de Galicia.

Fuente: cuenta oficial de Instagram de Banco de Galicia

Asimismo, dio lugar a que la Asociación de Bancos de la Argentina (ABA), la Asociación de Bancos Públicos y Privados de la Argentina (ABAPPRA), la Asociación de la Banca Especializada (ABE) y la Asociación de Bancos Argentinos (ADEBA) se uniesen para llevar a cabo una campaña a través de redes sociales para difundir mejores políticas de ciberseguridad.

También se generó cierta alerta por el robo de datos personales a través del *vishing*, una modalidad de *phishing* cada vez más común, que afectó, además de a la banca, a fondos de inversión y *traders* de criptodivisas.

Por último, cabe mencionar que, dentro de las finanzas, las criptomonedas fueron uno los objetivos principales de los cibercriminales en los países de

[5] Es un tipo de troyano que actúa abriendo una «puerta trasera» en el sistema y permite que un *hacker* tome el control remoto del equipo sin que usuario se dé cuenta.

América Latina. Las principales amenazas tuvieron su origen en el troyano W64/CoinMiner y el *malware* Riskware/CoinMiner.

4.2.2. Otros grandes ciberataques ocurridos en 2020

Además de los casos que sufrió la banca privada argentina, durante el año pasado también se produjeron una serie de ataques cibernéticos — en el segundo semestre — a diversos organismos públicos, que generaron especial preocupación a nivel nacional.

Secretaría de Estado de Seguridad y Orden Público del Gobierno de San Juan

A finales de julio, Comparitech — firma especializada en seguridad informática — descubría que una base de datos de la Secretaría de Estado de Seguridad y Orden Público de la provincia de San Juan, con información de 115.000 argentinos que solicitaron el permiso para circular durante el periodo de cuarentena, quedó expuesta durante dos semanas en su sitio web.

Si bien se alertó a la Dirección Nacional de Ciberseguridad, que agilizó la baja de la información el día 29 del mismo mes, se averiguó que parte de la base de datos fue captada por un *hacker* a través de un robot automatizado conocido como Meow.

Dirección Nacional de Migraciones

A principios del mes de septiembre, el Ministerio del Interior informaba de un ciberataque a la Dirección Nacional de Migraciones que, con motivo de la caída del servidor, ocasionó demoras en el ingreso y egreso al país.

De acuerdo con el documento de la denuncia penal presentada, el causante fue un tipo *ransomware* llamado Netwalker, que permitió al grupo de *hackers* bloquear el acceso a los datos sensibles almacenados y amenazar con su publicación a menos que se produjera un rescate de 76 millones de dólares.

Este nunca llegó a producirse ya que se logró contener la amenaza. Asimismo, se informó que tanto la infraestructura crítica como la información personal y corporativa que administra el organismo, no se vio afectada.

Agencia Nacional de Seguridad Vial

En noviembre, un nuevo ataque *ransomware* recayó en la Agencia Nacional de Seguridad Vial, dependiente del Ministerio de Transportes. Esta vez se vinculó a REvil — también conocido como Sodinokibi —, que, a diferencia del caso anterior, funciona como *Ransomware as a Service* (SaaS); esto es, un grupo que se encarga de la creación y el mantenimiento del código, y otro de su distribución.

Se estima que los atacantes habrían secuestrado 50GB de información de acuerdo con las capturas de pantalla difundidas en redes sociales por la empresa de ciberseguridad DarkTracer, obtenidas del blog de REvil.

5. Precios

Con relación a los precios de la ciberseguridad, es importante destacar que al tratarse de un sector en constante proceso innovador y que comprende una amplia gama de soluciones, estos varían de acuerdo con la tipología del cliente y sus necesidades específicas, así como de la empresa proveedora. Por esta razón, resulta complicado realizar un análisis detallado del coste de cada uno de los servicios de seguridad cibernética.

No obstante, cabe señalar que, al tratarse de un rubro altamente globalizado, es muy frecuente que los precios sean similares en todo el mundo, salvo posibles excepciones relativas a incidencias con los tipos de cambio respecto al país de origen.

Partiendo de esta premisa, se utiliza la base de datos de Zaask, empresa referente en la contratación de servicios profesionales para pequeñas y medianas empresas, con el objetivo de ofrecer una referencia al lector.

En primer lugar, el cálculo del precio ofrece distintas fórmulas según la contratación que haga el cliente, si bien estas suelen producirse de la siguiente manera:

- Precio por licencia: esto implica que la seguridad se circunscribe al uso de un determinado *software*. El coste máximo son 6.000€ al año; en algunos casos los servicios de asistencia no se incluyen.
- Previo por niveles: si bien dependen de las soluciones incluidas en el paquete, usualmente los precios no superan los 2.000€ al mes; algunas empresas ofrecen la opción de una tarifa anual con opción a descuentos.
- Precio por número de equipos o usuarios: 150€ mensuales sería el coste máximo.

Por otro lado, la misma fuente también ofrece la serie de datos relativos al coste de ciertos servicios puntuales del sector:

TABLA 8: PRECIO DE LAS SOLUCIONES Y SERVICIOS DE CIBERSEGURIDAD

Solución / Servicio	Precio	
Auditoría	400 - 3.500€	Los diagnósticos más simples revisan la configuración de redes wifi, cuentas de correo electrónico, antivirus y *firewall*; entre otras cosas. Por su parte, los más avanzados incluyen el análisis de tráfico en la red, test de intrusión, *hacking* ético y simulación de infecciones a través de *ransomware*.
Copia de seguridad	200 - 600€	Se pueden realizar tanto físicamente por medio de un disco duro, como con repositorios *online*.
Ciberseguro	350 - 1.200€ (anuales)	Existen diferentes coberturas; las más comunes son las siguientes: • Gestión de accidentes • Reclamación y daños a terceros por vulneración de la Ley de protección de datos • Indemnización por cese de actividad

Fuente: elaboración propia a partir de Zaask

6. Percepción del producto español

Cada año, el Real Instituto Elcano analiza la reputación de España en el mundo a partir de una muestra de más de 30.000 entrevistas en 55 países, entre los que se incluye Argentina. Entre las diferentes categorías que conforman el estudio, se incluye la percepción del producto español en distintas actividades económicas.

En el *Country RepTrak* del 2020, la sección de «Tecnología / Innovación» — incluye la ciberseguridad — muestra como los productos y servicios españoles obtuvieron una puntuación de 66,7 sobre 100.

TABLA 9: RANKING MUNDIAL DE LA PERCEPCIÓN DE «TECNOLOGÍA / INNOVACIÓN»

Posición mundial	País	Puntuación
1	Japón	89,6
2	Estados Unidos	79,6
3	Alemania	78,8
4	Suiza	78,7
5	Suecia	78,2
6	Singapur	78,1
7	Noruega	77,9
8	Finlandia	75,7
9	Reino Unido	75,6
10	Países Bajos	75,2
23	**España**	**66,7**
38	**Argentina**	**52,5**

Fuente: elaboración propia a partir del Real Instituto Elcano

Dicha puntuación fue prácticamente similar a la opinión que tienen los encuestados radicados en América Latina, tal y como se aprecia en la siguiente tabla:

TABLA 10: RANKING DE LA PERCEPCIÓN DE «TECNOLOGÍA / INNOVACIÓN» EN AMÉRICA LATINA

Posición	País	Puntuación
1	Japón	85,8
2	Estados Unidos	83,8
3	Alemania	80,9
4	China	79,4
5	Canadá	74,8
6	Reino Unido	74
7	Rusia	71,3
8	Francia	71,2
9	**España**	**66,9**
10	Italia	65,8
17	**Argentina**	**43,9**

Fuente: elaboración propia a partir del Real Instituto Elcano

Por otro lado, concretando en el caso de la opinión argentina, el informe también incluye la diferencia entre la valoración obtenida por el conjunto de países que conforman el G8 y varias de las regiones de América Latina. Como se puede observar, la tecnología española tiene una mejor reputación entre estas últimas, excepto en el caso de Brasil y Columbia:

TABLA 11: PERCEPCIÓN DE LA «TECNOLOGÍA / INNOVACIÓN» ESPAÑOLA: LATAM VS. G8

País	Puntación del país vs. G8
Perú	11%
México	7,2%
Chile	5,2%
Argentina	**1,4%**
Brasil	-1,7%
Colombia	-5,8%

Fuente: elaboración propia a partir del Real Instituto Elcano

Por último, cabe recordar lo visto en el apartado 3.3.2. respecto a la ciberseguridad española, la cual está considerada como la cuarta mejor del mundo por la ITU.

7. Canales de distribución

Los operadores del mercado argentino de la ciberseguridad ofrecen sus servicios a clientes de distinta índole. Por ello, se diferencian dos vías de acceso a cada uno de ellos.

En primer lugar, el cliente público utiliza el método de la licitación pública para satisfacer sus necesidades de soluciones de seguridad cibernética. Para obtener información sobre los concursos públicos — nacionales y provinciales — se puede recurrir a los siguientes canales:

TABLA 12: FUENTES INFORMACIÓN PARA LICITACIONES PÚBLICAS EN ARGENTINA

Fuente	Pública / Privada	Sitio web
COMP.AR	Pública	https://comprar.gob.ar/
CONTRAT.AR	Pública	https://contratar.gob.ar/
Boletín Oficial (*Sección Tercera*)	Pública	https://www.boletinoficial.gob.ar/seccion/tercera
InfoSICOES	Privada	https://www.argentinalicitaciones.com/
Diario de Licitaciones	Privada	http://www.diariodelicitaciones.com/

Fuente: elaboración propia a partir de varias páginas web

Para ampliar información sobre el sistema de licitaciones en Argentina, puede acceder al informe elaborado por esta Oficina Económica y Comercial, disponible en la sección Documentos y Estadísticas > Estudios e Informes de nuestra página web: www.argentina.oficinascomerciales.es.

Por otra parte, en relación con el cliente privado, se puede trazar una línea divisoria entre las grandes empresas y las pymes. Para el primer grupo, generalmente, las compañías cuentan con un proveedor de confianza, por lo que participar en sesiones de *networking*, así como en eventos y conferencias del sector supone ampliar las posibilidades de conseguir este tipo de contratos.

En el caso de las pymes, dependerá mucho de los recursos destinados a cubrir las necesidades de ciberseguridad. Igualmente, también recurrirán a la recomendación de su distribuidor habitual previo a la adquisición de una solución que se ajuste a la necesidad del momento.

Respecto a los distribuidores y *resellers*, muchos de ellos han aumentado su cuota de mercado gracias a otras del sector; por este motivo, normalmente existe un alto grado de fidelidad hacia estas marcas.

Por último, el usuario particular tiende a recurrir a los minoristas para contratar productos y servicios del rubro. Si bien, para ello, pueden acudir a las grandes superficies o a las tiendas locales, las plataformas *online* son sin duda alguna su principal vía para la compra.

8. Acceso al mercado – Barreras

Tal y como ocurren en gran parte de los sectores productivos en Argentina, la ciberseguridad es vulnerable a la incertidumbre política del país tras el cambio de gobierno en diciembre de 2019, así como a las crisis cíclicas de su economía. Por este motivo, resulta complicado llevar a cabo proyectos a medio y largo plazo en los que existen componentes de investigación y desarrollo.

8.1. Marco legislativo

8.1.1. Normativa

De acuerdo con la Dirección Nacional de Ciberseguridad, la normativa vinculada al sector incluye las siguientes leyes:

Ley 26.388 de Delito Informático

Esta norma tipifica nuevos delitos distintos a los incluidos en el Código Penal de la Nación. En ella, se incorporan sanciones para los siguientes casos:

- Intercepción, difusión y suspensión de cualquier tipo de comunicación electrónica
- Acceso ilícito a sistemas informáticos
- Acceso a bases de datos personales
- Propagación de virus informático
- Cometer fraude o causar daño informático

Ley 25.326 de Protección de Datos Personales

Tiene por objetivo garantizar el derecho a la intimidad de las personas mediante la protección integral de sus datos personales almacenados en archivos, registros, bases de datos u otros medios técnicos de tratamiento de datos, tanto públicos como privados.

Ley 25.506 de Firma Digital

Permite fijar las condiciones de uso, así como reconocer su eficacia jurídica, de la firma electrónica y la firma digital.

Ley 26.904 de *Grooming*

Regula este tipo de delito, castigado con penas que van desde 6 meses a 4 años, a los adultos que se contacten con menores de edad a través de algún medio electrónico, con el propósito de atentar contra la integridad sexual de estos.

Ley 27.126 de Inteligencia Nacional

Define el marco jurídico en el cual se llevan a cabo las actuaciones de inteligencia del Estado, conforme a la Constitución Nacional y los tratados de derechos humanos.

8.1.2. Organismos responsables

Principalmente, destacan los siguientes organismos responsables en materia de seguridad cibernética en el país:

Dirección Nacional de Ciberseguridad

Sus principales acciones comprenden la protección de las infraestructuras críticas de información, así como la generación de soluciones de prevención, detección, defensa, respuesta y recuperación ante incidentes de seguridad informática del Sector Público Nacional.

Oficina Nacional de Tecnologías de Información

Se encarga de dirigir la formulación de políticas e implementación del proceso de desarrollo e innovación tecnológica para la transformación e innovación del Estado Nacional. También promueve tanto la integración de nuevas tecnologías, como su compatibilidad e interoperabilidad.

División de Delitos Tecnológicos de la Policía Federal Argentina (PFA)

Tiene la obligación de investigar los casos de delitos informáticos y dispone de distintas competencias, dentro de las que está la de proporcionar información sobre la manera de detectar y comunicar ciberataques.

8.2. Tratamiento fiscal

Debido a su característica intangible, las soluciones de ciberseguridad no están sujetas a la retención en la Aduana, pero esto no implica que el importador argentino esté exento de los correspondientes costes tributarios.

Actualmente está vigente la Resolución 549 de la Administración Federal de Ingresos Públicos (AFIP), que establece que los importadores de este tipo de servicios, en la medida que se encuentren inscritos en el Impuesto al Valor Agregado (IVA), deben ingresar el 21 % en un plazo

de 10 días hábiles desde la generación del hecho imponible; es decir, desde el momento en que concluye la prestación del servicio[6].

En lo que respecta al exportador español, es importante mencionar que las operaciones de importación en Argentina también están sujetas a un anticipo del 6 % con cargo al Impuesto a las Ganancias (IG) — equivalente al Impuesto de Sociedades (IS) en España —, pues el importe abonado en territorio argentino bajo este concepto, se lo puede deducir en su siguiente declaración gracias al Convenio para Evitar la Doble Imposición vigente entre ambos países.

8.2.1. Aplicación del Convenio de Doble Imposición

Para ello, la empresa argentina debe tramitar la solicitud del certificado de retención ante la AFIP — equivalente a la Agencia Estatal de la Administración Tributaria (AEAT) en España — y remitirle la copia correspondiente a la empresa española.

Asimismo, el Convenio incluye un conjunto de tipos reducidos para ciertos servicios. Para poder beneficiarse de dicha aplicación, el importador argentino debe acreditar ante el banco, en el momento de pago, la condición de residente fiscal en España del exportador mediante el modelo que se recoge en el Anexo I de la Resolución General 2228/2007 de la AFIP.

También, es obligatorio que el contrato esté inscrito en el Instituto Nacional de la Propiedad Industrial (INPI) o en la Dirección Nacional de Derecho de Autor (DNDA), según el caso que corresponda.

Por último, cabe mencionar que toda documentación originaria de un Estado que vaya a ser presentada a las autoridades de otro debe contar con la Apostilla de La Haya.

[6] La ley también establece que este debe estar vinculado a alguna actividad que se encuentre gravada por el mismo tipo de tributo.

9. Perspectivas y oportunidades del sector

9.1. Perspectivas del sector

Debido a la pandemia, las perspectivas de crecimiento de la gran mayoría de actividades económicas se han visto muy afectadas. Sin embargo, otros sectores como el de la ciberseguridad, si bien han sufrido un impacto negativo, este ha sido menor; incluso, en este caso, se proyecta que el rubro continúe creciendo, tal y como se muestra en el apartado 3.1 del informe.

Si bien son varios los factores que dan razón a esto, el incremento del teletrabajo durante el año pasado resultó un hecho que contribuyó significativamente, pues millones de empleados que compartían y archivaban datos privados en una red no segura, se convirtieron en un blanco fácil para la comunidad de ciberdelincuentes.

Es por ello, que se espera que el sector se mantenga como un generador de empleo — tal y como se menciona también en el apartado previamente señalado —, que permita contar con mayor capital humano para combatir este tipo de vulnerabilidades que causan cifras millonarias en pérdidas año a año.

Con todo, para que estas oportunidades en el ámbito de la ciberseguridad cibernética — fruto del nuevo paradigma social y económico — puedan alcanzarse, es importante contar con el apoyo por parte del Estado, así como de los organismos sectoriales correspondientes.

9.2. Oportunidades del sector

9.2.1. Estrategia Nacional de Ciberseguridad

Previamente se mencionaba que en 2019 se aprobaba la Estrategia Nacional de Ciberseguridad, la cual establece los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del ciberespacio. Estos son:

1. Concientización del uso seguro del ciberespacio
2. Capacitación y educación en el uso seguro del ciberespacio
3. Desarrollo del marco normativo
4. Fortalecimiento de capacidades de prevención, detección y respuesta
5. Protección y recuperación de información del Sector Público

6. Fomento de la industria de la ciberseguridad
7. Cooperación internacional
8. Protección de las Infraestructuras Críticas nacional de información

9.2.2. Ley de Economía del Conocimiento

A finales de 2020, se aprobaba la Ley de Economía del Conocimiento a través del Decreto 1034, en lo que supone un impulso a la competitividad de varios servicios que se engloban dentro del sector de la ciberseguridad — especialmente el *software* —, así como la apertura de nuevos mercados, la generación de empleo y la transformación productiva de todas las empresas del rubro.

En este sentido, todas aquellas que se inscriban en este régimen, serán beneficiarias de las siguientes ventajas fiscales:

- Reducción segmentada del Impuesto de las Ganancias, según el tamaño de la empresa
- Rebaja de hasta el 70 % en las contribuciones patronales

Debido a que esta normativa es especialmente relevante para las soluciones y servicios *software*, le recomendamos ampliar información sobre este sector a través de la lectura del Estudio de Mercado del Software en Argentina elaborado por esta Oficina a finales del año pasado.

9.2.3. Acuerdos de colaboración

Acuerdo INCIBE – ICEX

En febrero del año pasado, el Instituto Nacional de Ciberseguridad (INCIBE) e ICEX España Exportación e Inversiones firmaron un acuerdo de colaboración con el objetivo de mejorar la competitividad española de esta industria, mediante la aceleración de empresas emergentes y el apoyo durante su proceso de expansión internacional.

Para ello, las principales acciones que llevarán a cabo de forma conjunta consisten en el desarrollo de misiones comerciales, tanto directas como inversas.

Acuerdo MINCyT – CDTI

El Ministerio de Ciencia, Tecnologías e Innovación de Argentina (MINCyT) y el Centro para el Desarrollo Tecnológico Industrial de España (CDTI) — en el marco del convenio de colaboración firmado en 2006 por ambas partes — acaban de anunciar este mes de junio una nueva «Llamada de Colaboración Tecnológica Empresarial Argentina-España».

Con esta acción, ponen a disposición de las empresas españolas y argentinas interesadas, una herramienta de financiación — coordinada y descentralizada — para fomentar proyectos de investigación y desarrollo tecnológico.

Para esta convocatoria se van a priorizar diversas áreas de actividad entre las que se encuentra la ciberseguridad. Asimismo, esta se estructura en dos fases, aunque es necesario superar la primera — cierra el próximo 29 de septiembre — para poder avanzar a la siguiente.

De resultar de su interés, puede ampliar la información sobre la convocatoria descargando aquí el fichero de la misma.

10. Información práctica

10.1. Ferias

Debido a la pandemia, desde el mes de marzo del año pasado y hasta nuevo aviso, en Argentina se ha suspendido prácticamente toda celebración de actos presenciales destinados a un gran número de público.

Sin embargo, los organizadores de alguno de estos eventos — ferias, congresos, etc. — han optado por mantener el calendario inicial y desarrollar los mismos de manera virtual; otros, en cambio, han preferido postergar la celebración a la espera de que en 2022 haya mejorado la situación sanitaria.

Respecto al sector de la ciberseguridad, la única feria anunciada de manera oficial hasta el momento es la siguiente:

Intersec Buenos Aires	
Fechas	24 al 26 de 55gosto de 2022
Sitio web	https://intersec-buenos-aires.ar.messefrankfurt.com/
Email	intersec@argentina.messefrankfurt.com
Teléfono	+54 11 4514 1400
Organización	Cámara Argentina de Seguridad Electrónica (CASEL), Cámara Argentina de Seguridad (CAS) y Messe Frankfurt

No obstante, es probable que próximamente se anuncien las fechas de la Pulso IT LIVE, que el año pasado celebró virtualmente su cuarta edición.

10.2. Asociaciones y cámaras profesionales

Asociación Argentina de Lucha Contra el Cibercrimen (AALCC)	
Dirección postal	Gurruchaga 485 C1414DHI – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.cibercrimen.org.ar/
Email	contacto@cibercrimen.org.ar
Teléfono	+54 9 11 5476 8369 / 5687 8461

Cámara Argentina de Seguridad Electrónica (CASEL)

Dirección postal	Moreno 957, Piso 4, Oficina 3 C1091AAS – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.casel.org.ar/
Email	info@casel.org.ar
Teléfono	+54 11 4331 6129 / 4342 1383

Cámara de la Industria Argentina del Software (CESSI)

Dirección postal	Marcelo T. de Alvear 636 C1058AAH – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.cessi.org.ar/
Email	info@cessi.org.ar
Teléfono	+54 11 5217 7802 / 7803 / 7804 / 7805

Cámara Argentina de Internet (CABASE)

Dirección postal	Suipacha 128 C1008AAD – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.cabase.org.ar/
Email	info@cabase.org.ar
Teléfono	+54 11 5263 7456

10.3. Otras direcciones de interés

Embajada de España en Buenos Aires

Dirección postal	Avda. Figueroa Alcorta 3102, Piso 1 C1425CKS – Ciudad Autónoma de Buenos Aires
Sitio web	http://www.exteriores.gob.es/embajadas/buenosaires
Email	emb.buenosaires@maec.es
Teléfono	+54 11 4809 4900

Oficina Económica y Comercial de España en Buenos Aires

Dirección postal	Avda. Figueroa Alcorta 3102, Piso 2 C1425CKS – Ciudad Autónoma de Buenos Aires
Sitio web	http://argentina.oficinascomerciales.es/
Email	buenosaires@comercio.mineco.es
Teléfono	+54 11 4809 4960

Consulado General de España en Buenos Aires

Dirección postal	Guido 1760 C1016AAE – Ciudad Autónoma de Buenos Aires
Sitio web	http://www.exteriores.gob.es/consulados/buenosaires
Email	cog.buenosaires@maec.es
Teléfono	+54 11 4814 9100

Consulado General de España en Bahía Blanca

Dirección postal	L.M. Drago 45, Piso 4, Oficina B – Edificio Torre Bicentenario B8000DCA – Bahía Blanca (Buenos Aires)
Sitio web	http://www.exteriores.gob.es/consulados/bahiablanca
Email	cog.bahiablanca@maec.es
Teléfono	+54 291 452 2549 / 3347

Consulado General de España en Córdoba

Dirección postal	Bulevar Chacabuco 875 X5000III – Córdoba
Sitio web	http://www.exteriores.gob.es/consulados/cordoba
Email	cog.cordoba@maec.es
Teléfono	+54 351 469 7490 / 8700

Consulado General de España en Mendoza

Dirección postal	Agustín Álvarez 455 M5500BAZ – Mendoza
Sitio web	http://www.exteriores.gob.es/consulados/mendoza
Email	cog.mendoza@maec.es
Teléfono	+54 261 42 3947

Consulado General de España en Rosario

Dirección postal	Santa Fe 768 S2000ATH – Rosario (Santa Fe)
Sitio web	http://www.exteriores.gob.es/consulados/rosario
Email	cog.rosario@maec.es
Teléfono	+54 341 447 0100

Cámara Española de Comercio en la República Argentina (CECRA)

Dirección postal	Belgrano 863, Piso 7 C1092AAI – Ciudad Autónoma de Buenos Aires
Sitio web	http://www.cecra.com.ar
Email	recepcion.cecra@cecra.com.ar
Teléfono	+54 11 4335 5000

Dirección Nacional de Ciberseguridad

Dirección postal	n/a
Sitio web	https://www.argentina.gob.ar/direccion-nacional-ciberseguridad
Email	administracionciberseguridad@jefatura.gob.ar
Teléfono	+54 11 3984 900 (Ext. 7127)

Instituto de Ciencias e Ingeniería de la Computación (ICIC)

Dirección postal	San Andrés 800 – Universidad Nacional del Sur B8000CTX – Bahía Blanca (Buenos Aires)
Sitio web	https://icic.conicet.gov.ar/
Email	dir.icic@cs.uns.edu.ar
Teléfono	+54 291 459 5101 / 2611

Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BA-CSIRT)

Dirección postal	n/a
Sitio web	https://www.ba-csirt.gob.ar/
Email	ciberseguridad@ba-csirt.gob.ar
Teléfono	+54 11 4323 9362

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

Dirección postal	Sarmiento 663, Piso 6 C1041AAM – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.mpf.gob.ar/ufeci/
Email	denunciasufeci@mpf.gov.ar
Teléfono	+54 11 5071 0040 / 0041

Ministerio de Ciencia, Tecnología e Innovación

Dirección postal	Godoy Cruz 2320 C1425FQD – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.argentina.gob.ar/ciencia
Email	info@mincyt.gob.ar
Teléfono	+54 11 4899 5000

Ministerio de Seguridad
Argentina

Ministerio de Seguridad	
Dirección postal	Gelly y Obes 2289 C1425EMA – Ciudad Autónoma de Buenos Aires
Sitio web	https://www.argentina.gob.ar/seguridad
Email	denuncias@minseg.gob.ar
Teléfono	+54 11 5278 9800

11. Bibliografía

AALCC (2020). *La Argentina encabeza un peligroso ranking del cibercrimen*. Disponible en https://www.cibercrimen.org.ar/2020/10/09/la-argentina-encabeza-un-peligroso-ranking-del-cibercrimen/?utm_source=email_marketing&utm_admin=17774&utm_medium=email&utm_campaign=El_de_los_ciberataques_son_a_travs_del_mail

Agencia EFE (2021). *Los delitos informáticos se disparan en Argentina a raíz de la pandemia*. Disponible en https://www.efe.com/efe/espana/sociedad/los-delitos-informaticos-se-disparan-en-argentina-a-raiz-de-la-pandemia/10004-4506944

Alfaro, P. (2021). *La ciberseguridad escala puestos en la agenda mundial*. Disponible en www.tendencias.kpmg.es/2018/01/la-ciberseguridad-escala-puestos-en-la-agenda-mundial/

BOE (2013). *Convenio entre el Reino de España y la República Argentina para evitar la Doble Imposición y prevenir la evasión fiscal en materia de impuestos sobre la renta y sobre el patrimonio*. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2014-373

Casas, X. (2020). *Economía del Conocimiento: el sector celebró la quita de retenciones y pronostica un alto impacto positivo en la exportación de servicio*. Disponible en https://www.infobae.com/economia/2020/12/21/economia-del-conocimiento-el-sector-celebro-la-quita-de-retenciones-y-pronostica-un-alto-impacto-positivo-en-la-exportacion-de-servicios/

CCN-CERT (2020). *Ciberamenazas y tendencias. Edición 2020.*

CDTI (2021). *Convocatoria 2021: Llamada bilateral Argentina-España para la financiación de proyectos empresariales de investigación y desarrollo tecnológico*. Disponible en https://www.cdti.es/recursos/doc/Programas/Cooperacion_internacional/Iberoeka/Argentina/34606_1061062021134423.pdf

Ceteri, J.L. (2018). *Importaciones de servicios: qué costos tributarios afrontan*. Disponible en https://www.cronista.com/columnistas/Importaciones-de-servicios-que-costos-tributarios-afrontan-20181115-0059.html/

CEPAL (2020). *La ciberseguridad en tiempos de la COVID-19 y el tránsito hacia una ciberinmunidad*. Disponible en https://www.cepal.org/sites/default/files/publication/files/46275/S2000679_es.pdf

Ciberseguridad.com (2021). *Empresas de ciberseguridad en Argentina*. Disponible en https://ciberseguridad.com/empresas/argentina/

CISCO (2018). *Cibersecurity Annual Report.*

Cybermap Kaspersky (2021). Disponible en https://cybermap.kaspersky.com/es

CyberSecurity News (2020). *El estado de la ciberseguridad en Latinoamérica 2020: Brasil y México los países más ciberatacados*. Disponible en https://cybersecuritynews.es/el-estado-de-la-ciberseguridad-en-latinoamerica-2020-brasil-y-mexico-los-paises-mas-ciberatacados/

Davidovsky, S. (2020). *Un ataque ransomware amenaza con publicar información privada de la Agencia Nacional de Seguridad Vial*. Disponible en https://www.lanacion.com.ar/tecnologia/un-ataque-ransomware-amenaza-publicar-informacion-privada-nid2521829/

Enfasys (2021). *Más de 900 millones de intentos de ciberataques afectaron a Argentina en 2020*. Disponible en https://www.enfasys.net/2021/02/26/mas-de-900-millones-de-intentos-de-ciberataques-afectaron-a-argentina-en-2020/

Enfasys (2021). *Argentina sufrió más de 187 millones intentos de ciberataques entre enero y marzo de 2020*. Disponible en https://www.enfasys.net/2020/05/05/argentina-sufrio-mas-de-187-millones-intentos-de-ciberataques-entre-enero-y-marzo-de-2020/

Fortinet (2021). *Fortinet consolida su liderazgo en el 2020 con 53 % de cuota de mercado en número de dispositivos de ciberseguridad vendidos en América Latina y el Caribe*. Disponible en https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/fortinet-consolida-liderazgo-en-2020-de-dispositivos-de-ciberseguridad-en-america-latina

Gartner (2020). *Gartner forecasts worldwide security and risk management spending to exceed $150 billion in 2021*. Disponible en https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Gobierno de la República Argentina (2019). *Estrategia Nacional de Ciberseguridad de la República Argentina*. Disponible en https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf

Gobierno de la República Argentina (2021). *Normativa – Ciberseguridad*. Disponible en https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

González, M. (2021). *Ley de la Economía del Conocimiento: ya se aprobó, empecemos a usarla*. Disponible en https://www.infobae.com/opinion/2021/01/03/ley-de-la-economia-del-conocimiento-ya-se-aprobo-empecemos-a-usarla/

IADB (2020). *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*.

IBM (2021). *X-Force Threat Intelligence Index 2021*.

INAP (2021). Disponible en https://capacitacion.inap.gob.ar/

INCIBE (2016). *Tendencias en el mercado de la ciberseguridad.*

INCIBE (2020). *INCIBE e ICEX se unen para promover la internacionalización de la industria española de ciberseguridad*. Disponible en https://www.incibe.es/sala-prensa/notas-prensa/incibe-e-icex-se-unen-promover-internacionalizacion-industria-espanola

Infobae.com (2020). *Eliminaron las retenciones a las exportaciones de servicios basados en el conocimiento*. Disponible en https://www.infobae.com/economia/2020/12/21/eliminaron-las-retenciones-a-las-exportaciones-de-servicios-basados-en-el-conocimiento/

Infobae.com (2020). *La información de 115 mil personas que tramitaron el permiso de circulación quedó expuesta en la red por una falla de seguridad*. Disponible en https://www.infobae.com/sociedad/2020/08/07/la-informacion-de-115-mil-personas-que-tramitaron-el-permiso-de-circulacion-quedo-expuesta-en-la-red-por-una-falla-de-seguridad/

Infotechnology.com (2020). *Vishing: la nueva estafa financiera que es más peligrosa que el Phishing*. Disponible en https://www.infotechnology.com/online/Vishing-la-nueva-estafa-financiera-que-es-mas-peligrosa-que-el-Phishing-20200825-0010.html

Infotechnology.com (2021). *Explotaron las estafas bancarias en Argentina: hay 3000 % más tarjetas y homebankings en peligro*. Disponible en https://www.infotechnology.com/actualidad/en-la-argentina-las-denuncias-por-estafas-bancarias-crecieron-3000-como-protegerse/

International Trade Administration (2020). *Argentina Cybersecurity*. Disponible en https://www.trade.gov/market-intelligence/argentina-cybersecurity

Inversor Latam (2020). *Los bancos de Argentina son el objetivo principal de los ciberataques en el país*. Disponible en https://inversorlatam.com/los-bancos-de-argentina-son-el-objetivo-principal-de-los-ciberataques-en-el-pais/

Iproup.com (2021). *Nuevos ataques a las empresas: más de 900 millones de intentos de ciberataques afectaron a la Argentina en 2020*. Disponible en https://www.iproup.com/economia-digital/21031-ciberseguridad-900-millones-de-ataques-afectaron-al-pais-en-2020#:~:text=Los%20resultados%20obtenidos%20en%20la,de%20ataques%20en%20el%20pa%C3%ADs

ITU Publications (2018). *Global Cybersecurity Index*. Disponible en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITware Latam (2020). *Aumenta el cibercrimen en Argentina*. Disponible en https://www.itwarelatam.com/2020/05/08/aumenta-el-cibercrimen-en-

argentina/#:~:text=Argentina%20sufri%C3%B3%20m%C3%A1s%20de%20187,de%20ciberseguridad%20a%20nivel%20global

ITware Latam (2020). *Entre julio y septiembre en Argentina se registraron 84 millones de intentos de ciberataque*. Disponible en https://www.itwarelatam.com/2020/11/13/entre-julio-y-septiembre-en-argentina-se-registraron-84-millones-de-intentos-de-ciberataques/

Jaimovich, D. (2020). *Hackearon la Agencia Nacional de Seguridad Vial y amenazan con difundir la información*. Disponible en https://www.infobae.com/tecno/2020/11/27/hackearon-la-agencia-nacional-de-seguridad-vial-y-amenazan-con-difundir-la-informacion/

Kaspersky (2021). *¿Qué es la ciberseguridad?* Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lavoz.com (2020). *Cuáles son las ciberamenazas para Argentina en el 2020*. Disponible en https://www.lavoz.com.ar/tecnologia/cuales-son-ciberamenazas-para-argentina-en-2020/#:~:text=Un%20tipo%20de%20ransomware%20%22m%C3%A1s,2020%20por%20una%20empresa%20de

Microsoft (2021). *Ciberseguridad en las empresas de Argentina*.

Mordor Intelligence (2021). *Latin American cybersecurity market – growth, trends, COVID-19 impact, and forecasts 2021-2026*. Disponible en https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

Morgan, S. (2020). *Top 5 cybersecurity facts, figures, predictions and statistics for 2020 to 2021*. Disponible en https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/

Mundo Ciruja (2021). *Informe de mercado (2021): Estrategia de jugadores clave, Análisis FODA - Pronóstico hasta 2030*. Disponible en http://mundociruja.com/ciberseguridad-crecimiento-anual-de-la-industria/

OEA (2019). *Desafíos del riesgo cibernético en el sector financiero en América Latina*.

Oficina Económica y Comercial de España en Buenos Aires (2021). *Sistema de licitaciones en Argentina*.

Oficina Económica y Comercial de España en Buenos Aires (2021). *Costes de una importación en Argentina*.

Paleo, M. (2021). *El año de los ciberataques: cómo hicieron los bancos argentinos para defender a sus clientes*. Disponible en https://www.infotechnology.com/mundo-cio/el-ano-de-los-ciberataques-como-hicieron-los-bancos-argentinos-para-defender-a-sus-clientes/

Real Instituto Elcano (2020). *La reputación de España en el mundo. Country Reptrak 2020.*

Rodríguez, M. (2020). *IDC asegura que el gasto mundial en ciberseguridad alcanzará los 174.700 millones de dólares*. Disponible en https://www.cloudmasters.es/idc-asegura-que-el-gasto-mundial-en-ciberseguridad-alcanzara-los-174-700-millones-de-dolares-sabias-que/

Silvestrini, J. (2021). *Tus cuentas bancarias y tus datos, en peligro: mirá los fraudes y estafas que se usan para sacarte todo por la web*. https://www.iproup.com/innovacion/16570-fraude-estafas-ciberataques-como-actua-la-ciberdelincuencia

Statista (2021). *Cybersecurity: leading vendors by market share 2020*. Disponible en https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share/

Threat Map Check Point (2021). Disponible en https://threatmap.checkpoint.com/

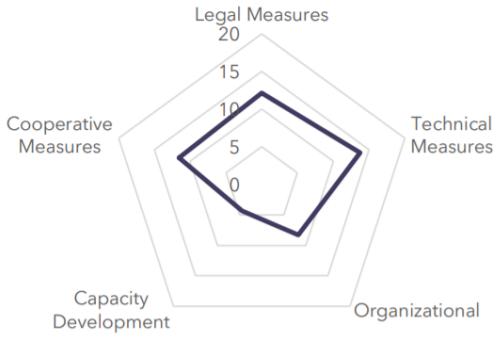
Welivesecurity.com (2016). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. Disponible en https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Williams, S. (2020). *Gartner: Spending on information security and risk management to continue to grow in 2020*. Disponible en https://itbrief.asia/story/gartner-spending-on-information-security-and-risk-management-to-continue-to-grow-in-2020

Zaask (2021). *Cuánto cuesta un servicio de ciberseguridad*. Disponible en https://www.zaask.es/cuanto-cuesta/ciberseguridad

12. Anexos

12.1. Anexo I – Global Cybersecurity Index: Argentina



Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
50.12	12.15	13.75	8.29	4.38	11.55

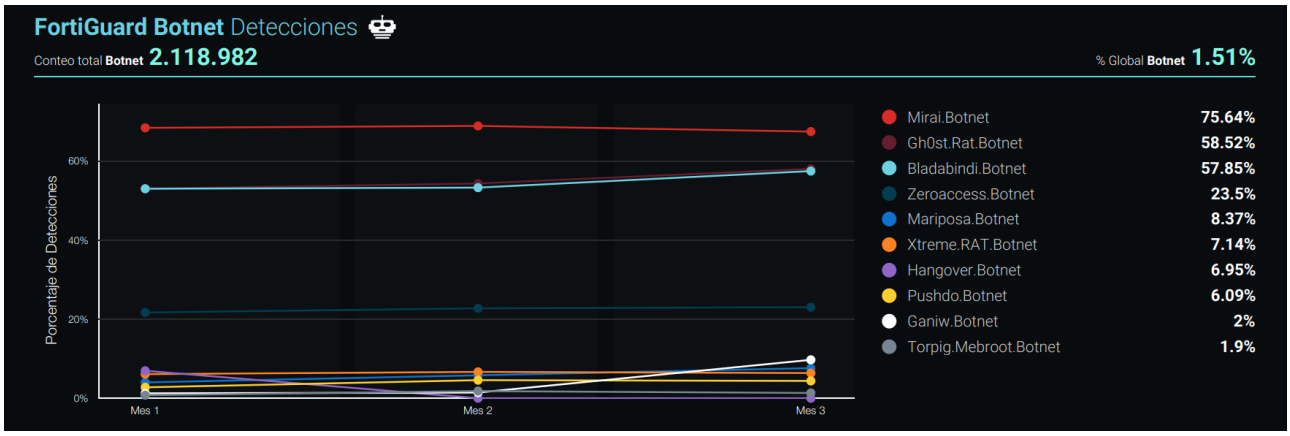
Fuente: ITU

12.2. Anexo II – Amenazas registradas durante el 4º trimestre de 2020

Virus

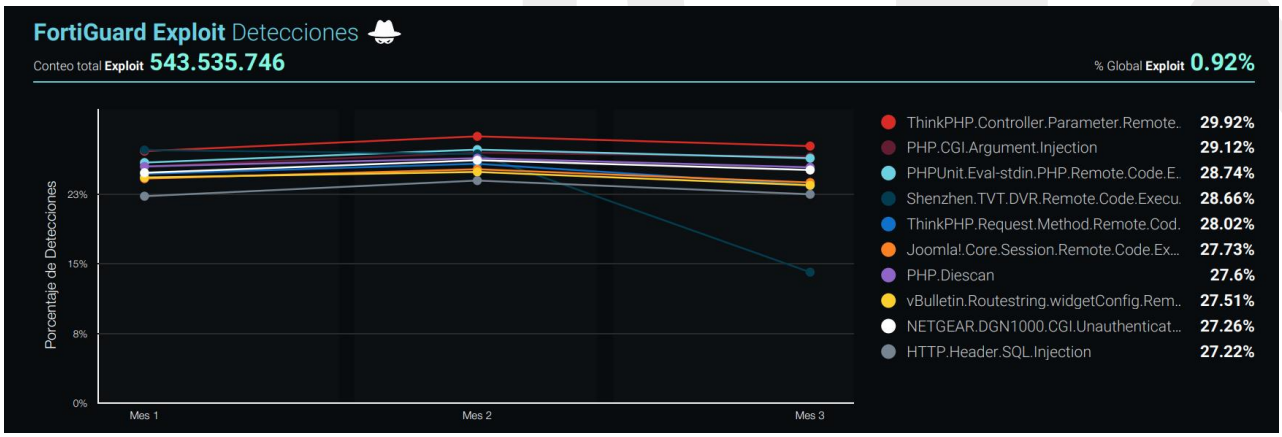
Fuente: FortiGuard Labs

Botnet



Fuente: FortiGuard Labs

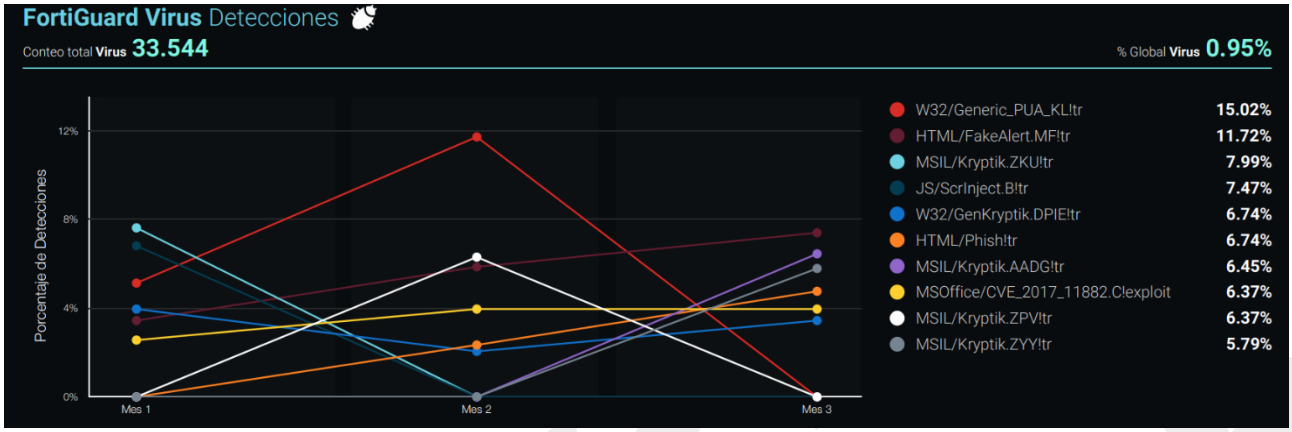
Exploit



Fuente: FortiGuard Labs

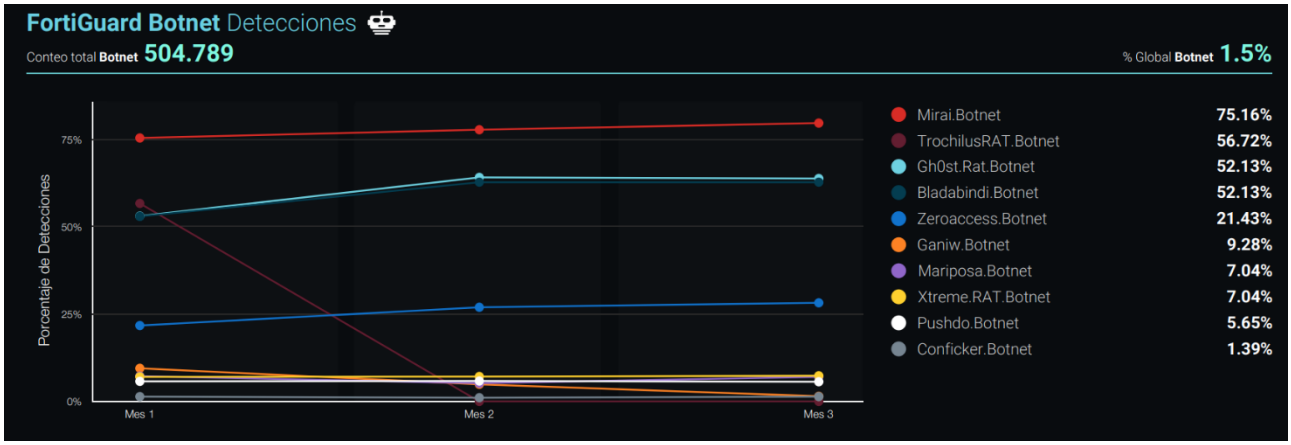
12.3. Anexo III – Amenazas registradas durante 1er trimestre de 2021

Virus



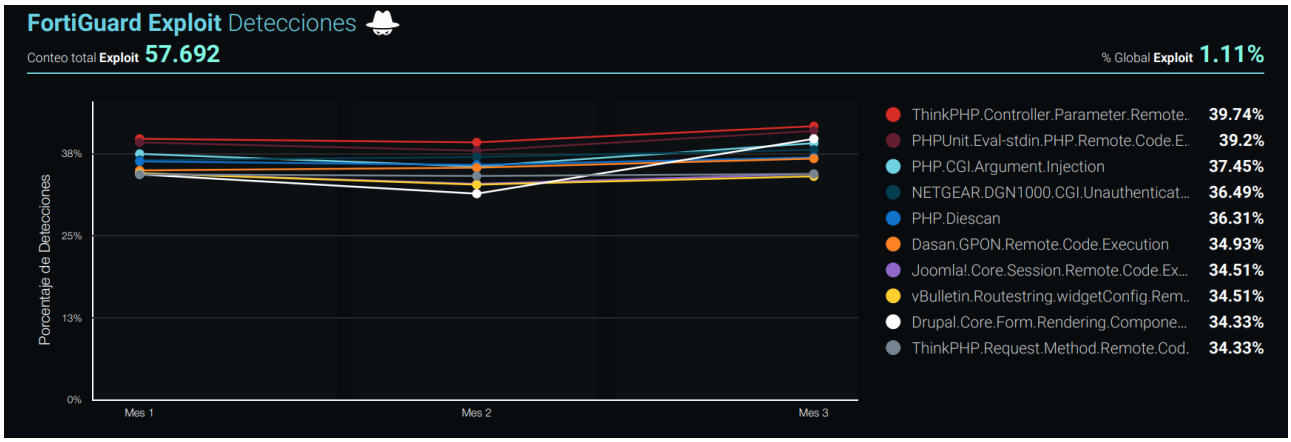
Fuente: FortiGuard Labs

Botnet



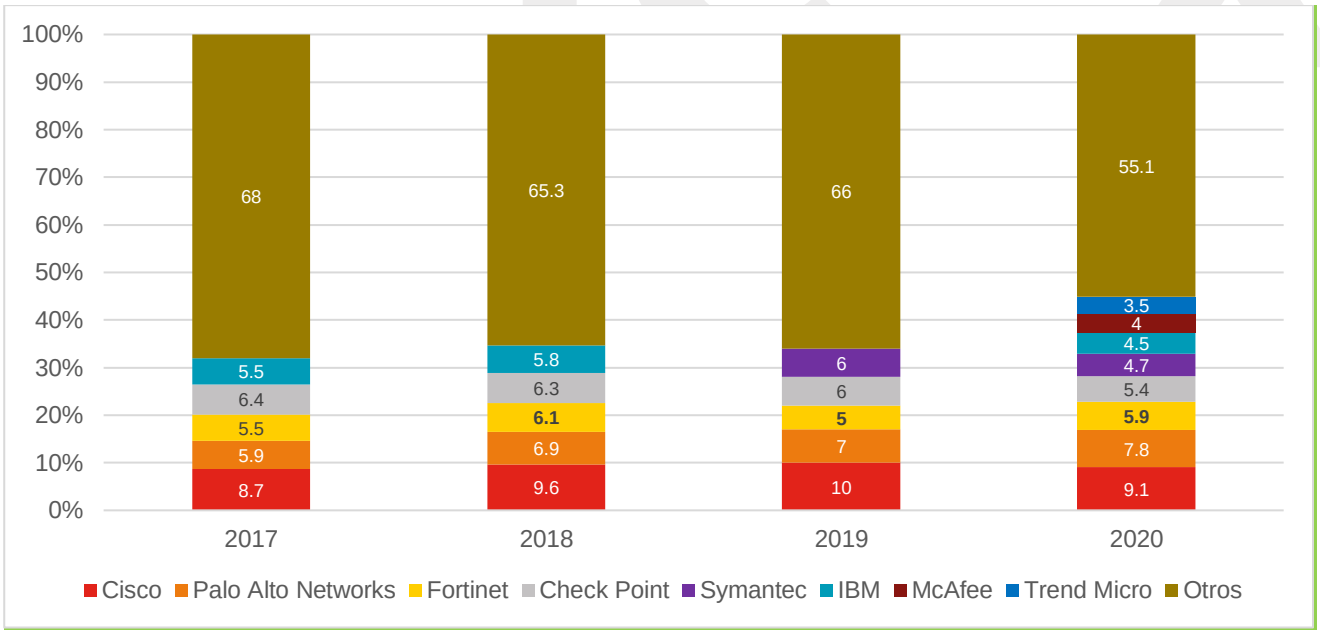
Fuente: FortiGuard Labs

Exploit



Fuente: FortiGuard Labs

12.4. Anexo IV – Cuota de mercado mundial de las principales empresas de ciberseguridad (2017 - 2020)



Fuente: elaboración propia a partir de Statista

Si desea conocer todos los servicios que ofrece ICEX España Exportación e Inversiones para impulsar la internacionalización de su empresa contacte con:

Ventana Global
913 497 100 (L-J 9 a 17 h; V 9 a 15 h)
informacion@icex.es

Para buscar más información sobre mercados exteriores siga el enlace

www.icex.es

EM

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
ICEX España Exportación e Inversiones