Cámara Argentina de Comercio y Servicios

Índice de Intensidad Digital

Marzo 2024

Director:
Carlos Pirovano

Coordinador:
Sebastián Ferrari

Investigadores:
María Victoria Armellini
Julio César Rodriguez Rabellini
María Emilia Rey Saravia

Cada vez son más las empresas que reconocen la necesidad de implementar herramientas de Ciberseguridad (63%)

- El 55% de las empresas utilizan herramientas de monitoreo en forma remota (Internet de las Cosas)
- El 68% de las empresas que utilizan Fintech lo hacen desde Mercado Pago
- Sigue en aumento el porcentaje de empresas que analiza o explota big data internamente (36%)

Elaborado por

Observatorio de Productividad y Competitividad
Universidad CAECE
Cámara Argentina de Comercio y Servicios

Contacto:
observatorio@caece.edu.ar

Con el apoyo de

MERCADO ARGENTINO DE VALORES S.A.

ZOFINGEN

ÍNDICE

¿Por qué un IID?

- La Cámara Argentina de Comercio y Servicios (CAC), a través del Observatorio de Productividad y Competitividad (OPyC) de la Universidad CAECE, elabora el Índice de Intensidad Digital, referido a la adopción de tecnologías por parte de las empresas argentinas.
- El objetivo central es estudiar, evaluar y monitorear el estado de digitalización de los procesos de negocio implementados por las firmas analizadas. Para ello se indaga en diversas cuestiones referidas al uso de herramientas como el e-Commerce, la infraestructura en la nube, las redes sociales y tecnologías emergentes (como big data e inteligencia artificial), entre otros aspectos.
- Para el diseño del indicador, se siguieron los lineamientos de diversos reportes elaborados por la Unión Europea, con vasta experiencia en mediciones de estas características.
- La realización del presente estudio es posible gracias a los aportes financieros de las empresas que lo acompañan:

Sponsors

MERCADO ARGENTINO DE VALORES S.A.

ZOFINGEN

La ciberseguridad es un desafío para todas las organizaciones

Por Santiago Cavanna – Chief Information Security Officer (CISO) de Microsoft Sudamérica HSP

Así de crudo, así de cierto

La ciberseguridad es una prioridad para los directores de las empresas más importantes. Esta prioridad se traduce en decisiones estratégicas que impactan en la cultura, pero también en la tecnología, los procesos y las políticas.

Esto que es cierto para las organizaciones más grandes, no necesariamente lo es para el resto.
Las estadísticas tampoco son alentadoras, con el avance de la tecnología, la transformación también llega a las organizaciones criminales, que encuentran tierra fértil para alcanzar sus objetivos. De hecho, se han vuelto mucho más eficaces, diversificándose, alcanzando cobertura global, subcontratando u ofreciendo servicios a otras organizaciones criminales o simplemente ofreciendo sus servicios cual mercenarios.

Hay al menos 300 grupos organizados alrededor del globo que llevan adelante actividades criminales, algunos de ellos con raíces en Latinoamérica, pero todos con incidencia global.

Se duplicaron los casos de ransomware durante 2023 y el 70% de las organizaciones afectadas tienen menos de 500 empleados. Todo esto lo pueden ver en el reporte anual de Microsoft, de Octubre de 2023.

Todo esto es preocupante, pero también es cierto que la experiencia de los últimos años permite entender tanto vectores de ataque como posibles vías de mejora en la postura y aumento de resiliencia en las organizaciones. Esto aplica a organizaciones de todos los tamaños, y tiene nombre propio: confianza cero. Pero hay más, las recomendaciones de ciber higiene, ponen en evidencia que hay espacio de mejora en la manera en la que las organizaciones gestionan la tecnología que hace de soporte a los procesos de negocio.

Es posible, afirma Microsoft y yo comparto, reducir el 99% de la superficie de ataque que podría aprovechar alguno de esos actores criminales para convertirlo en su próxima víctima.
No debe sorprenderle que para estas organizaciones criminales, su organización es un objetivo, siempre y cuando el costo de atacarlo sea menor que el riesgo de ser atrapado y el monto del rescate que pueda obtener a cambio de devolverle el control de sus sistemas o eliminar la información exfiltrada.

Estar dos pasos por delante, salirse de grupo objetivo, romperle el modelo de negocio al atacante, es posible, está al alcance de su organización e incluso, es probable que este dentro del presupuesto de Tecnología.

La ciberseguridad es un desafío para todas las organizaciones

Confianza cero, un paradigma de ciberseguridad

La confianza cero es un modelo de seguridad que se basa en el principio de que ninguna entidad, interna o externa, es de fiar por defecto. Esto implica que se debe verificar la identidad, el contexto y el comportamiento de cada usuario, dispositivo y solicitud antes de otorgar el acceso a los recursos de la organización.

La confianza cero busca reducir la superficie de ataque, limitar el movimiento lateral de los atacantes y mejorar la visibilidad y el control de la red. Para implementar la confianza cero, se requiere de una serie de componentes, como:

- Una política de acceso basada en el mínimo privilegio, que solo otorgue el acceso necesario para cumplir una función específica.
- Una autenticación multifactorial, que combine diferentes factores de verificación, como la contraseña, el código PIN, el reconocimiento biométrico o el token.
- Una segmentación de la red, que divida la red en subredes más pequeñas y aisladas, con reglas de firewall y encriptación para cada una.
- Una monitorización continua, que recoja y analice los datos de la red, los usuarios, los dispositivos y las aplicaciones, para detectar y responder a las amenazas en tiempo real.

También es posible que escuche frases como “Asumir la brecha” en la práctica significa que tiene que imaginar que el compromiso, que el ataque es posible más allá de las medidas que ha tomado y, por lo tanto, tiene que lograr que el impacto sea el menor posible.

Aca quiero decir algo polémico, incómodo y poco feliz. Debe considerar incluso que algún miembro de su organización podría estar dispuesto a colaborar con alguna organización criminal a cambio de dinero. Esto ya ha ocurrido en la región de la mano de una de estas organizaciones criminales con raíces locales, lamentablemente modelo de exportación adoptado hoy día, por otras organizaciones en otras regiones.

Ciber higiene: un conjunto de buenas prácticas

La ciber higiene es el conjunto de buenas prácticas que las organizaciones deben seguir para mantener un nivel adecuado de seguridad en sus sistemas y datos. La ciber higiene implica tanto acciones preventivas como correctivas, que abarcan desde la gestión de las contraseñas hasta la actualización de los parches de seguridad

Algunas de las recomendaciones de ciber higiene son:

- Crear y cambiar las contraseñas con frecuencia, usando combinaciones de letras, números y símbolos, y evitando usar la misma contraseña para diferentes cuentas o servicios.

.

La ciberseguridad es un desafío para todas las organizaciones

- Realizar copias de seguridad de los datos importantes, tanto en dispositivos externos como en la nube, y verificar que se puedan restaurar correctamente.
- Instalar y actualizar los programas antivirus, antimalware y firewall, y configurarlos para que realicen escaneos periódicos y bloqueen las conexiones sospechosas.
- Actualizar los sistemas operativos y las aplicaciones, instalando los parches de seguridad que corrigen las vulnerabilidades que podrían ser explotadas por los atacantes.
- Educar y concienciar a los empleados sobre los riesgos y las amenazas de la ciberseguridad, y establecer unas normas y protocolos de actuación.

Parece obvio, pero no lo es. El grado de obsolescencia tecnológica que observo en muchas empresas no tiene justificación más allá de la falta de prioridad, o músculo para hacer las migraciones, lo urgente le gana a lo importante y cada vez se hace más difícil estar al día.

Note que nada de lo dicho antes, tiene un impacto real en su presupuesto, pero sí tiene impacto en la priorización de las tareas o en el modelo de rendición de cuentas de las áreas de seguridad y tecnología, las métricas, en última instancia los incentivos o penalidades.

Tan relevante se ha vuelto este último punto, el de rendición de cuentas, que en Julio de 2023 la SEC (security & exchange comission) organismo que supervisa a las empresas locales o extranjeras que cotizan en la bolsa de los Estados Unidos, modificó las reglas que aplican a los supervisados, exigiéndoles que hagan explícito el modelo de gestión de riesgos ciber para que asumieran responsabilidad desde el directorio y luego también la obligación de que reportaran cualquier incidente de ciberseguidad con impacto material que pudiera afectar a los accionistas minoritarios que operan en el mercado.

Conclusión

La ciberseguridad es un desafío y una oportunidad para las organizaciones, que deben adaptarse a un entorno cada vez más complejo y dinámico. La confianza cero y la ciber higiene son dos conceptos clave para mejorar la seguridad de los activos y los procesos de negocio, y requieren de un compromiso y una inversión por parte de los directivos y los empleados. La ciberseguridad no es solo una cuestión técnica, sino también una cuestión estratégica, cultural y humana.

No importa el tamaño de su organización, ni la dependencia tecnológica de sus procesos de negocios. Debe comprender que opera en un contexto peligroso y aunque no está solo, debe hacer su parte.

Fraudes Digitales

Por BTR Consulting

El 50% de las violaciones de ciberseguridad involucraron EL ROBO DE CREDENCIALES, estas son empleadas en mayor proporción para lanzar ataques de ransomware dirigidos a grandes y medianas empresas, incluidas las organizaciones gubernamentales. Para obtener estas credenciales, los atacantes utilizan principalmente técnicas de PHISHING, y en la misma galería de delitos se presentan como variantes para continuar confundiendo al mercado y sus víctimas, Vishing, Anuncios Fraudulentos-AdWords, Cuento del Tío Digital y Skimming Online, entre otros.

De acuerdo a un estudio realizado por nuestro Extreme Cybersecurity Lab, un 69% de los incidentes que generan un daño económico, se realizan a través de plataformas tecnológicas, incluyendo sitios de redes sociales, mensajería y servicios de eCommerce.

El conocimiento y tecnología para la comisión de ciberdelitos están disponibles y son gratuitos.

El ciberdelito, es una industria que tiene más recursos y presupuesto que Gobiernos, Agencias de Seguridad, Justicia y Entidades Financieras.

El factor humano es el comportamiento de los usuarios como motor del ciberdelito, más allá de la prevención, de la necesidad de educar y concientizar. Los ciberdelincuentes están teniendo cada vez más en cuenta el comportamiento de los usuarios para dirigir sus ataques. Se basan más en técnicas de ingeniería social, la situación de incertidumbre, se añade a que muchos usuarios se muestran muy preocupados por la protección de su identidad digital y no creen ser capaces de poder detectar una amenaza.

Casi el 70% de los CIBERATAQUES tienen motivaciones económicas, seguidos por el robo de propiedad intelectual, identidad de terceros y ciber espionaje.

Sin embargo, las diferentes modalidades de PHISHING, RANSONWARE, y LOS COMPROMISOS DE CORREO ELECTRÓNICO, incluyen aumentos en la cantidad de ataques que involucran diferentes técnicas como el “CUENTO DEL TÍO”; ROBO, CLONACIÓN Y SUPLANTACIÓN DE IDENTIDAD, VIOLACIÓN DE DATOS PERSONALES, y la combinación más efectiva en todos los frentes, ESTAFAS rematadas por WhatsApp,

Ejemplos de diferentes técnicas de estafas utilizadas por WhastApp:

- Estafas de WhatsApp Bussiness
- Estafas de números equivocados de WhatsApp
- Engaño de verificación
- Suplantación de identidad/La estafa de mamá, papá, familia, amigo, etc.
- Secuestro de WhatsApp
- Hackeo de correo de voz

Aplicación comprometida, versiones de WhatsApp no oficiales

- Links dañinos

Fraudes Digitales

- Estafa de criptomonedas de WhatsApp
- Complete la encuesta
- Videollamada extorsiva

El auge de la Inteligencia Artificial aporta herramientas que ayudan a los ciberdelincuentes a limpiar el lenguaje. Abriendo así nuevas puertas para que los piratas informáticos entren en las redes a través de correos electrónicos que engañan a los destinatarios para que compartan información personal.

La importancia de considerar la educación a una empresa sobre ciberseguridad

Los usuarios, ya sean como individuos o en su rol de empleados en organizaciones, siguen siendo el motor del ciberdelito. Más allá de la prevención, la educación y la concientización son esenciales.

Si promovemos una cultura de ciberseguridad podremos desarrollar organizaciones robustas y menos vulnerables a ciberataques.

Cerca del 95% de los incidentes de ciberseguridad en organizaciones que implican fuga de datos o pérdida de privacidad tienen que ver con un error humano.

Los riesgos cibernéticos se consideran uno de los principales peligros globales para la economía en su conjunto. La frecuencia y gravedad de los ciberataques son cada vez mayores; las filtraciones de datos para robar información personal y profesional ocurren a diario, pero solo las más grandes son noticias.

Cómo prevenirlos

Algunas recomendaciones que podés adecuar a tu día a día laboral y personal:

- NO hagas click en enlaces sospechosos ni descargues archivos de correos electrónicos no solicitados.
- ACTUALIZÁ regularmente tu software de seguridad y sistema operativo.
- UTILIZÁ CONTRASEÑAS FUERTES y cambiálas periódicamente.
- EDUCÁ a los miembros de tu equipo o familia sobre amenazas cibernéticas y la importancia de la precaución online.
- REPORTÁ cualquier actividad sospechosa.
- Si usás alguna herramienta de Inteligencia Artificial, no tomés decisiones basadas exclusivamente en resultados generados por IA, sin la intervención de criterio humano. Todos los resultados obtenidos de herramientas de IA, deben ser validados (y ajustados) previo a su utilización final.
- No cargues información altamente confidencial y/o sensible de la compañía, ni personal en ChatGPT o cualquier otro sistema de chat con IA, ya que podría generar daño reputacional, pérdida de competitividad y otras contingencias legales. Recordá que la información ingresada puede almacenarse para un uso posterior, lo que podría ocasionar Fuga de Datos.

Recordá que la seguridad es responsabilidad de todos. Tomar medidas proactivas para proteger tu información personal y profesional es esencial en un entorno digital cada vez más complejo.

De inversionistas, "influencers" y grandes riquezas digitales fáciles

Por Iván Alexander Gawek - Analista de Inteligencia focalizado en cibercrimen y fraude

Multiplicar el dinero que poseemos siempre es y será una interesante oferta para un trabajador promedio. Qué tal si a eso le agregamos la posibilidad de hacerlo empleando unos pocos minutos diarios y a través de una aplicación móvil desde el sillón de casa, el colectivo o una pausa del trabajo. Sumemosle, entonces, la facilidad de acceder con descuento y algún regalo más, si podemos sumar un par de "colaboradores" a este increíble negocio que nos ofrece ganancias en USD y/o cripto activos e inversiones de increíbles rendimientos y retornos del 30% al 100% anual (sí, ofrecen esa cifra, mientras que el rendimiento promedio anualizado de los últimos tres años de Treasury Bond Floating Rate del Tesoro de los Estados Unidos, ha sido del 3.13% 1). Imposible rechazar, además, esto que es ofrecido por un personaje que nos demuestra su éxito a través de la exhibición – no poco obscena - de relojes exclusivos, autos deportivos de colores chillones, ropa de marcas peculiares, viajes por paraísos y cenas propias de las élite de otros tiempos. La oferta se completa con la posibilidad de transformar no solo su economía y finanzas personales, ofreciendo libertad absoluta financiera - aún trato de entender qué es esto - si no también la persona: serás una mujer invencible, o un hombre sigma, no andarás en chiquitajes, hay un mundo exclusivo y privativo para todos aquellos que sean capaces de aventurarse para dejar atrás su antiguo ser, de mentalidad pobrista y sistémica, para dar nacimiento a un humano nuevo, eficiente, potente, indómito y millonario. Y todo eso por una mínima suma mensual y el uso de esta plataforma de trading, que usted usará desde hoy y sin necesidad de aprender muchos más que estos 10 videos (si tan solo supieron que fácil es esos Quants que se han doctorado en matemática luego de 10 años de costoso estudio). ¿Quién puede dudar - además- si eso es ofrecido por el presidente de un famoso banco de inversiones mundial, o una empresa de servicios digitales de esas que utilizamos diariamente?. Esta descripción, que parece salida de una performance del querido Tato Bores 2, es un escenario común de estafas y fraudes digitales que tienen como objetivo un público abrumado por la pérdida de valor de su salario en un escenario de alta inflación mundial, hiperconectividad y poder de las imágenes, donde ya resulta una tarea de altísimo nivel de investigación discernir que es real y que no.

La gran oferta de billeteras virtuales, plataformas de inversión, productos financieros para salvaguardar el valor de nuestros activos, la necesidad de disminuir el esfuerzo en un escenario de mayor productividad y estancamiento del ingreso del trabajador promedio (si trabajamos mejor, no, no ganamos mucho más, si, la vida es más cara hoy) 3, sumado a la gran oferta de productos y servicios deseables a consumir, son un marco propicio para el crecimiento del fraude y la estafa, si agregamos además, que desarrollar se ha vuelto más sencillo y menos de nicho - escribo esto no solo como analista de cibercrimen, si no también como programador -

De inversionistas, "influencers" y grandes riquezas digitales fáciles

nos encontramos con las condiciones necesarias ideales para que los que desean vivir del esfuerzo ajeno puedan llevar a cabo sus fechorías pudiendo empezar, sin demasiado esfuerzo, a atrapar a los que están con la guardia más baja, recaudar sumas de dinero interesantes y retirarse del negocio durante un tiempo sin dejar rastro alguno.

Para salir de la opinión en ingresar en el mundo de las métricas, dejo acá algunos números:

- Según el Federal Trade Commission, en 2023, 4.6 millones fueron comprometidos en fraude de falsas inversiones (solo en Estados Unidos).
- AML Intelligence, expresa que en 2023, en América (sin distinción), el fraude a través de plataformas de pagos comprometió USD 102.6 millones, compartiendo esta metodología el primer puesto tanto en EMEA y como en APAC.
- El FBI afirmó recientemente, que las pérdidas de inversiones relacionadas con las criptomonedas aumentaron de 2,57 mil millones de dólares en 2022 a alrededor de 3,94 mil millones de dólares en 2023, lo que representa un aumento del 53%.

Veamos como afecta esto a Latinoamérica y por que es un lugar propicio para el establecimiento de este tipo de “negocios” espurios:

- La región posee un grado considerable de adopción de internet y conectividad, en torno al 72% de su población se encuentra enlazada.
- Dada su distribución demográfica, más del 70% de la población promedio de los países que la componen, es urbana. Es decir, con un alto nivel de concentración.
- Alto ratio de inflación (promedio de región en 14%) y pérdida de valor del salario.
- Pobreza y desigualdad en altos niveles de registro.

De lo expuesto anteriormente se puede concluir, que la atracción de víctimas con el mensaje de incrementar ganancias de manera pasiva y mantener el valor del salario e ingresos, la facilidad de la viralización de estas ofertas, la accesibilidad al alcance de la mano, y la ingeniería social como técnica de obtención de información y focalización-segmentación del público (víctima), continuará “in-crescendo” para el año en curso. Debe sumarse a esto, la aparición de la IA para uso masivo a través de prompts de texto, imágenes, deep fakes, etc, como incremento de las capacidades de los estafadores, la venta de métodos de fraude y estafa en, ya no solo la internet profunda, si no abiertamente en plataformas de mensajes y redes sociales.

¿Qué veremos en 2024? En continuación de lo que hemos visto en los últimos 3 años, podemos distinguir las siguientes tendencias:

1. Avances impulsados por IA propulsan la tecnología deepfake, que utiliza inteligencia artificial para crear contenido falso convincente, como audio, video o imágenes, lo que representa una amenaza para la identidad y la seguridad empresarial.

De inversionistas, "influencers" y grandes riquezas digitales fáciles

2. La detección del robo de identidad sintética se vuelve más difícil, ya que combina elementos auténticos con información falsa, complicando los esfuerzos de prevención.

3. Se observa un aumento significativo en el fraude de usurpación de cuentas, con un incremento del 350% desdee 2020, lo que subraya la urgencia de proteger proactivamente a los clientes y adoptar medidas preventivas.

4. Las empresas son más vulnerables al fraude de tarjetas no presentes, ya que la proliferación del comercio electrónico crea oportunidades para que los estafadores exploten vulnerabilidades en sistemas de pago en línea.

5. Se eleva el riesgo de fraude interno, con un aumento del 44% en amenazas internas en los últimos años, lo que destaca la importancia de implementar controles internos y una cultura ética sólida.

6. Los ataques de ingeniería social están en aumento en la era del trabajo remoto, aprovechando la falta de conciencia de seguridad de los empleados que trabajan desde casa.

7. La proliferación de ciberdelincuencia como servicio (CaaS) facilita la participación de individuos con habilidades técnicas limitadas en actividades delictivas en línea.

8. La escasez de habilidades en ciberseguridad contribuye a la escalada de amenazas cibernéticas, destacando la necesidad de abordar esta brecha mediante la externalización, capacitación y retención de talento en ciberseguridad.

Finalmente, y desde el lado empresario del mostrador, el panorama de fraudes muestra una combinación de innovación y explotación de vulnerabilidades, exigiendo una respuesta proactiva para protegerse contra las amenazas digitales emergentes, principalmente, aquellas que ofrezcan servicios de pago digital, inversiones y rendimiento. Resulta imperioso centrarse en aquellas amenazas que proliferan en redes sociales y plataformas de comunicación tales como impostores (de ejecutivos y de la marca), robo de identidades de clientes, campañas de fraude y robo de credenciales basadas en emails (phishing), mensajes de texto (smishing) e impostores mediante llamadas (vishing). Procurar un activo monitoreo de las contestaciones en redes sociales de falsos empleados de atención al cliente, aplicaciones clonadas en mercados de aplicaciones e impostores de “gurúes financieros” que aleguen conexiones con la marca. Reforzar esto con una estrecha comunidad entre competidores de mercado, coadyuvará a la reducción del riesgo, las pérdidas de dinero por parte de la empresa y la reducción del ilícito que golpea, principalmente, a los más vulnerables.

Resumen ejecutivo

- **5,42** es el índice de Intensidad Digital de las empresas en Argentina.

Acceso y uso de internet

- **91%** de los entrevistados cuenta con acceso a Internet, con una velocidad de descarga que mayoritariamente fluctúa en dos rangos: entre 30 y 100mb, y entre 100 y 500mb.
- **61%** de las empresas proveen a sus empleados dispositivos portátiles con conexión móvil.
- **73%** dispone de website, al cual se le brinda un uso estático (descripción de bienes, servicios, precios (**66%**)) o como canal de venta (e-commerce) (**34%**).

E-Commerce

- **40%** efectúa ventas online a través de marketplaces.
- En el segundo semestre de 2023, **60%** de las ventas (promedio) fue por e-commerce.
- Entre los que realizaron ventas online, **70%** efectuó ventas a consumidores finales.
- **38%** realizó ventas de bienes o servicios a través de EDI-Type y dirigiéndose mayoritariamente a consumidores radicados en Argentina.

Intercambio de información electrónicamente dentro de la empresa

- **44%** dispone de un CRM orientado a funciones comerciales y **40%** cuenta con una plataforma enfocada a marketing.

Uso de servicios de computación en la nube

- **40%** adquirió servicios de computación en la nube.
- Los usos otorgados a la nube se vinculan esencialmente con el almacenamiento de datos (**54%**), emailing (**48%**), base de datos de la empresa en la nube (**43%**) y programas de seguridad (**43%**).

Internet de las Cosas (IoT)

- **55%** utiliza dispositivos interconectados de monitoreo remoto.
- **36%** analiza o explota big data internamente desde cualquier fuente de datos.

Inteligencia Artificial (IA)

- **34%** no utiliza tecnologías-herramientas de IA.
- Las herramientas de IA se emplean actualmente esencialmente para marketing y ventas (**40%**). En un segundo plano sobresale el uso para asistir a los clientes con respuestas automáticas (**38%**), logística (**24%**), procesos de administración (**24%**) y gestión de empresas (**21%**).

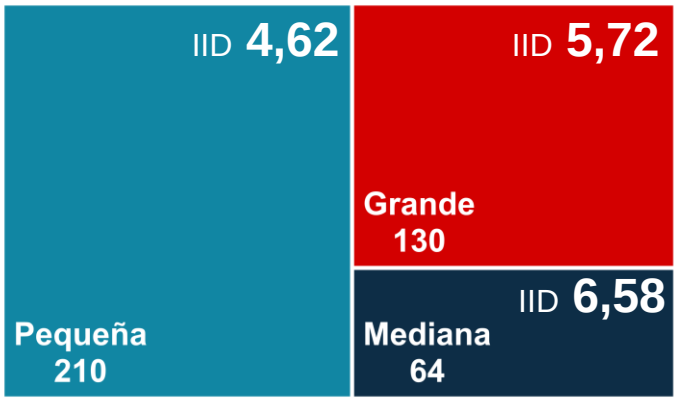
El Índice en Argentina

Índice de Intensidad Digital | Argentina 2023

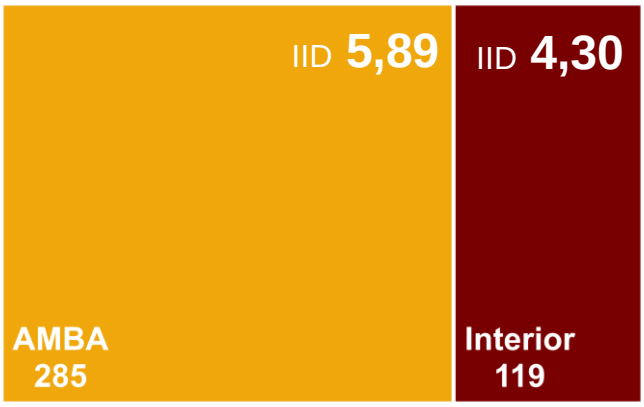
5,42
En una escala del 0 al 10

Muestra: 404
Promedio n° respuestas: 351

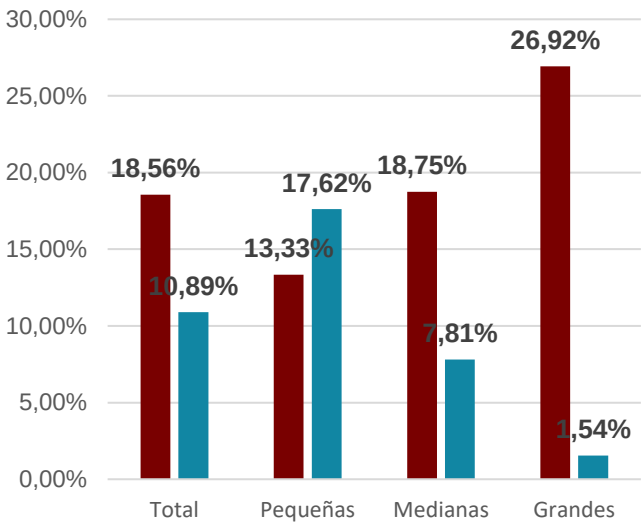
Por tipo de empresa

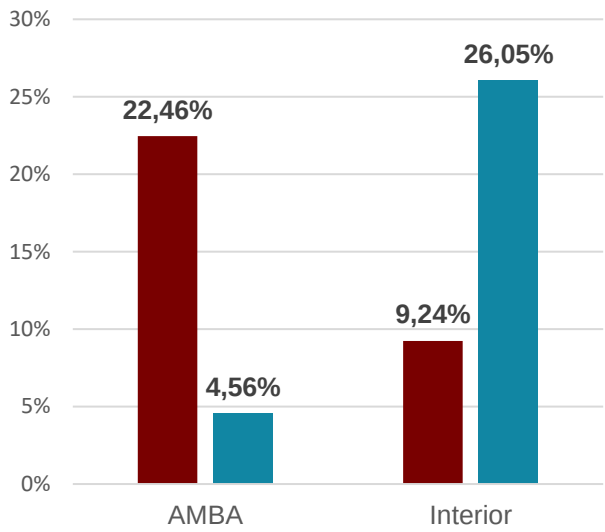


Por ubicación de la empresa



Análisis de valores extremos del IID





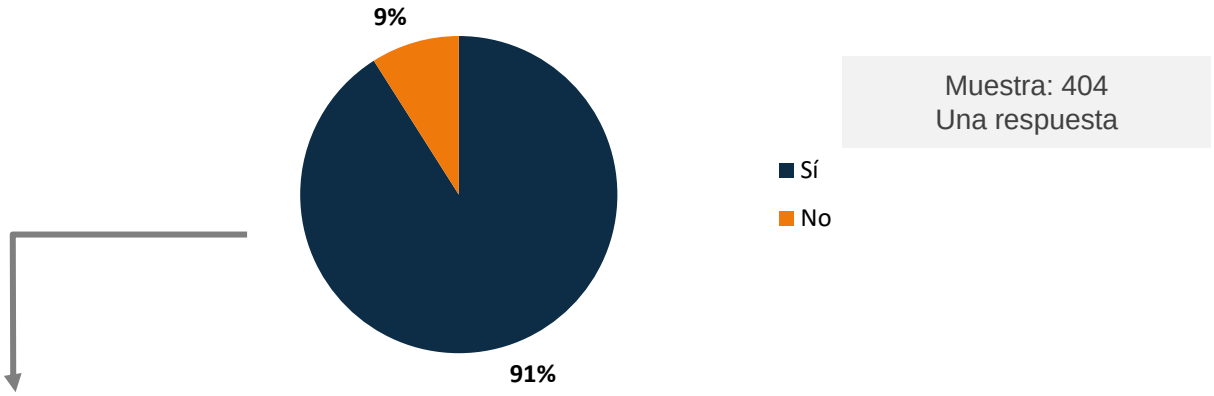
IID > 8
IID < 2

El Índice en Argentina

A- ACCESO Y USO DE INTERNET

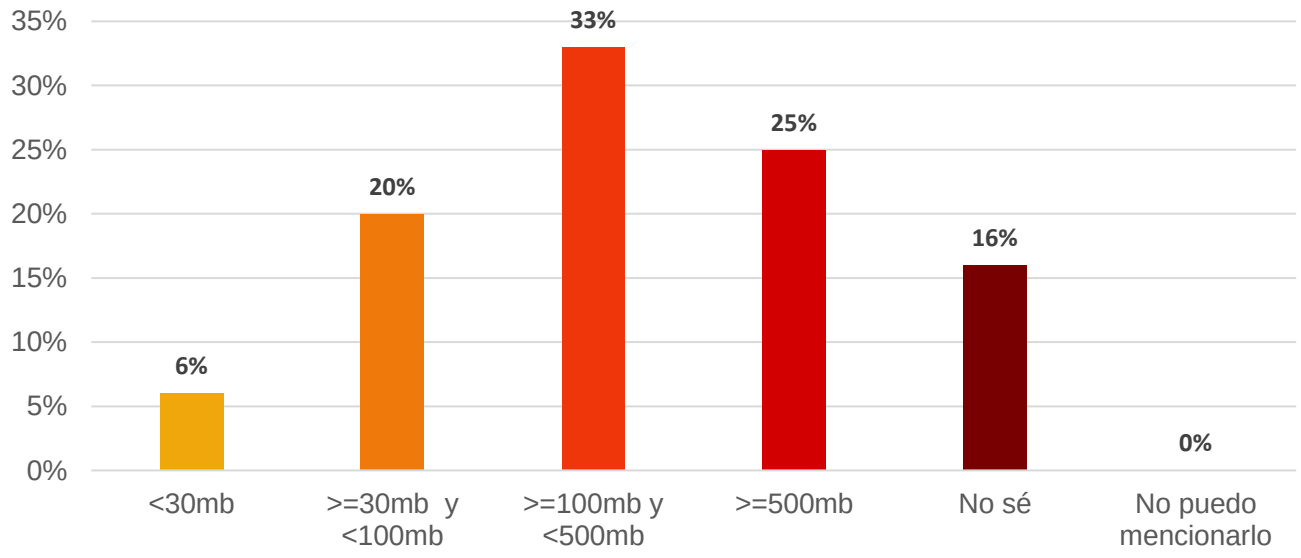
- **76%** (933 sobre 1307) empleados promedio tienen acceso a internet para fines comerciales.

Cantidad de empresas que utilizan algún tipo de conexión fija de Internet.



Muestra: 404
Una respuesta

Máxima velocidad de descarga contratada en la empresa.

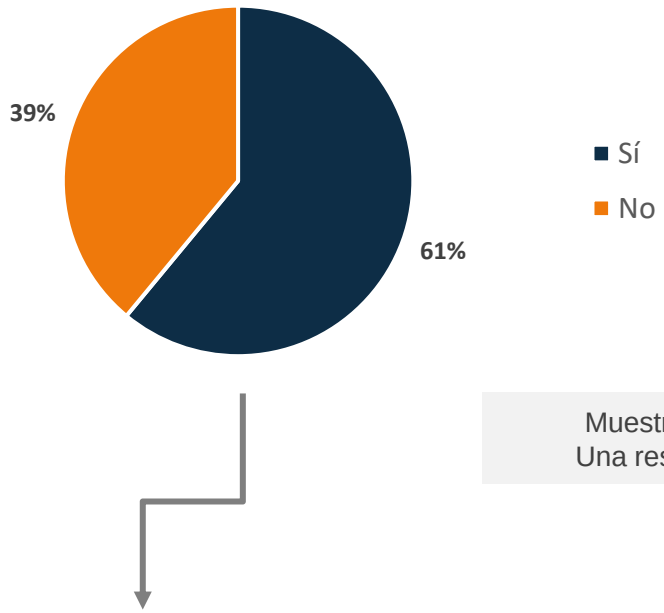


Muestra: 366
Respuesta múltiple

El Índice en Argentina

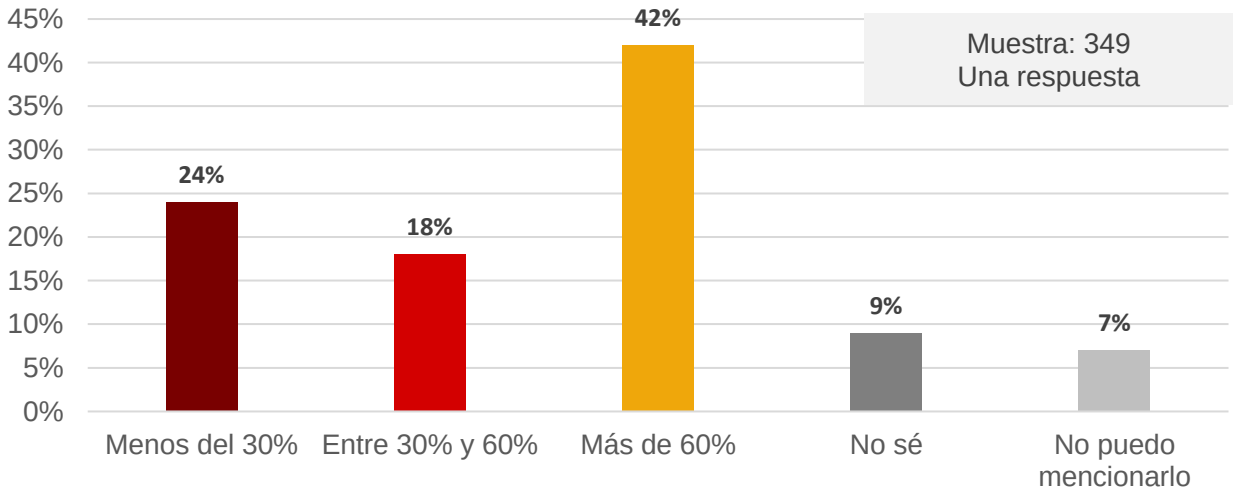
A- ACCESO Y USO DE INTERNET

Empresas que proveen a sus empleados dispositivos portátiles que permiten una conexión móvil a partir de redes de telefonía móviles, para fines comerciales.



Muestra: 404
Una respuesta

Porcentaje de empleados que usan un dispositivo portátil provisto por la empresa con conexión a internet móvil

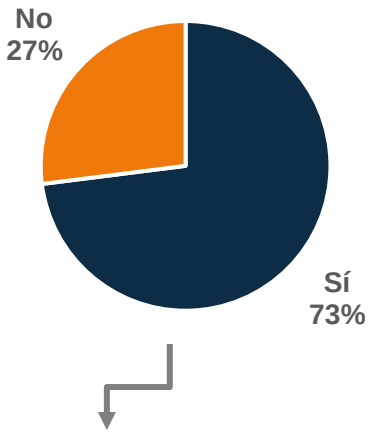


Muestra: 349
Una respuesta

El Índice en Argentina

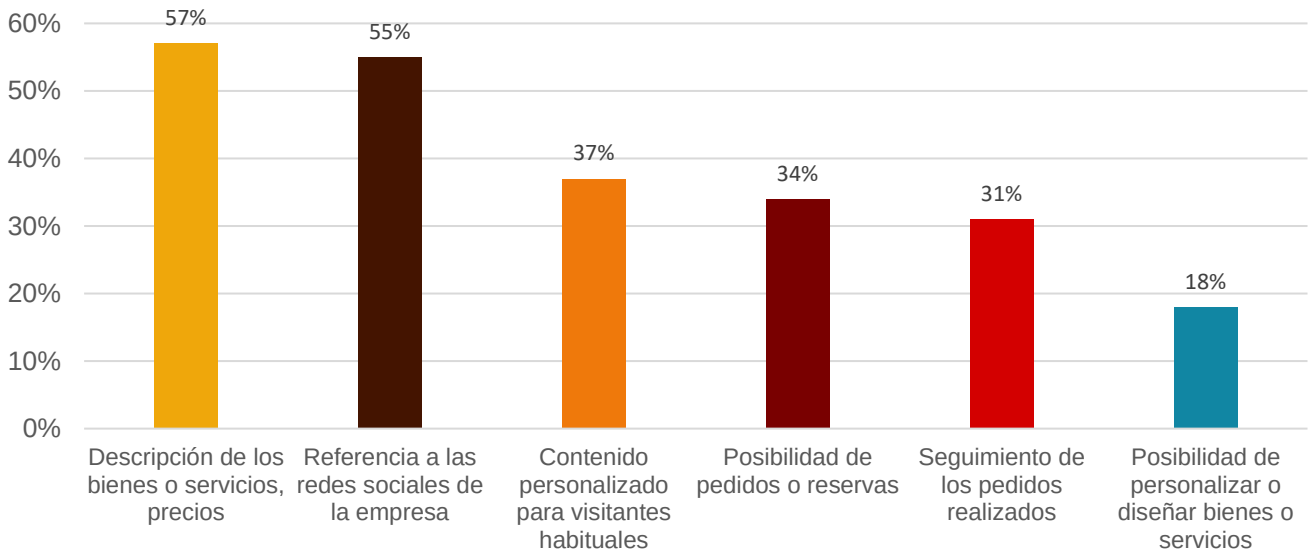
A- ACCESO Y USO DE INTERNET

Empresas que tienen sitio web.



Muestra: 404
Una respuesta

Funcionalidades que tienen los sitios web de las empresas.

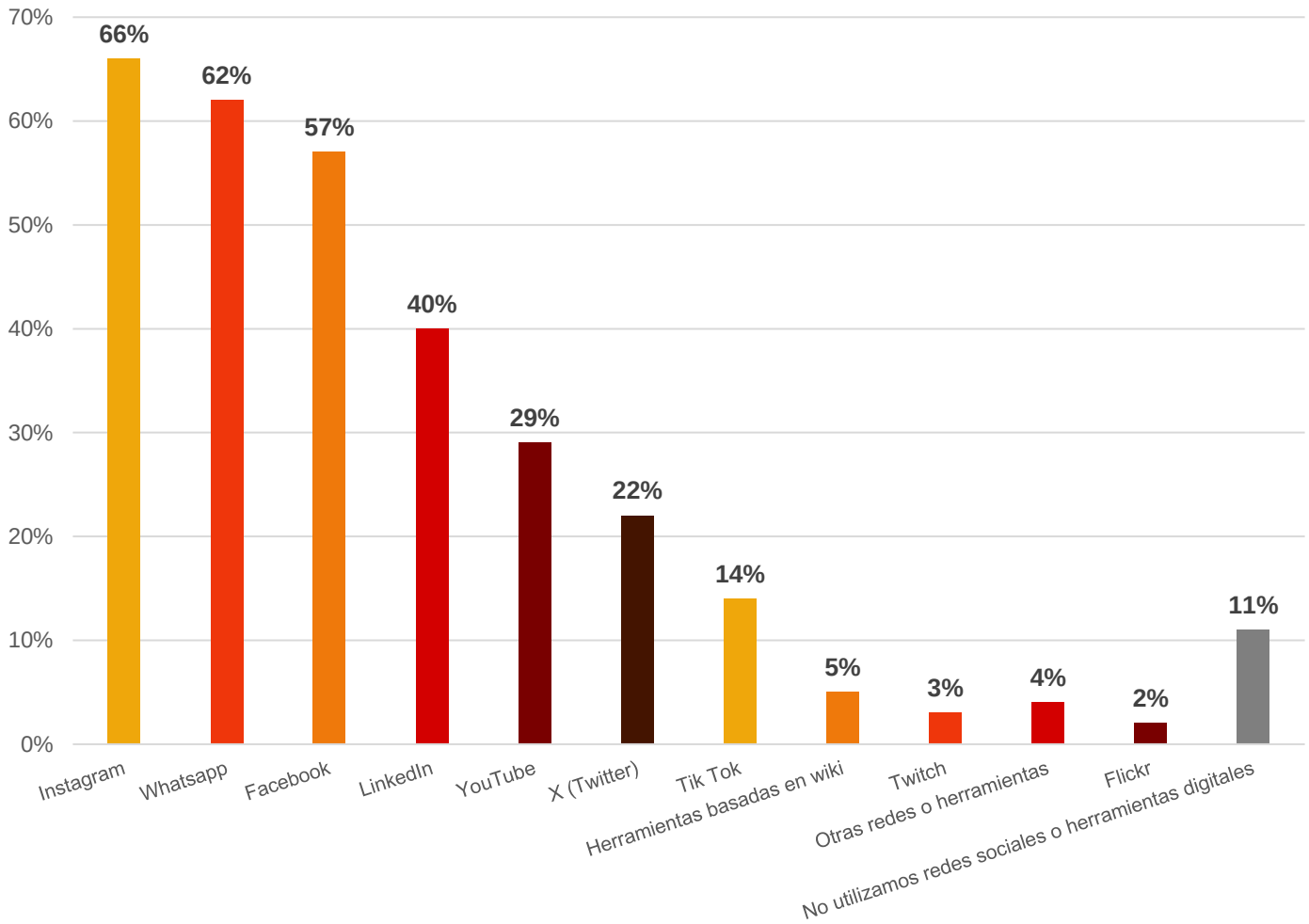


Muestra: 356
Respuesta múltiple

El Índice en Argentina

A- ACCESO Y USO DE INTERNET

Redes sociales y herramientas digitales que utilizan las empresas.



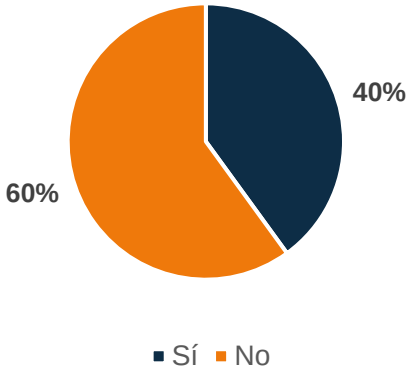
Muestra: 404
Respuesta múltiple

El Índice en Argentina

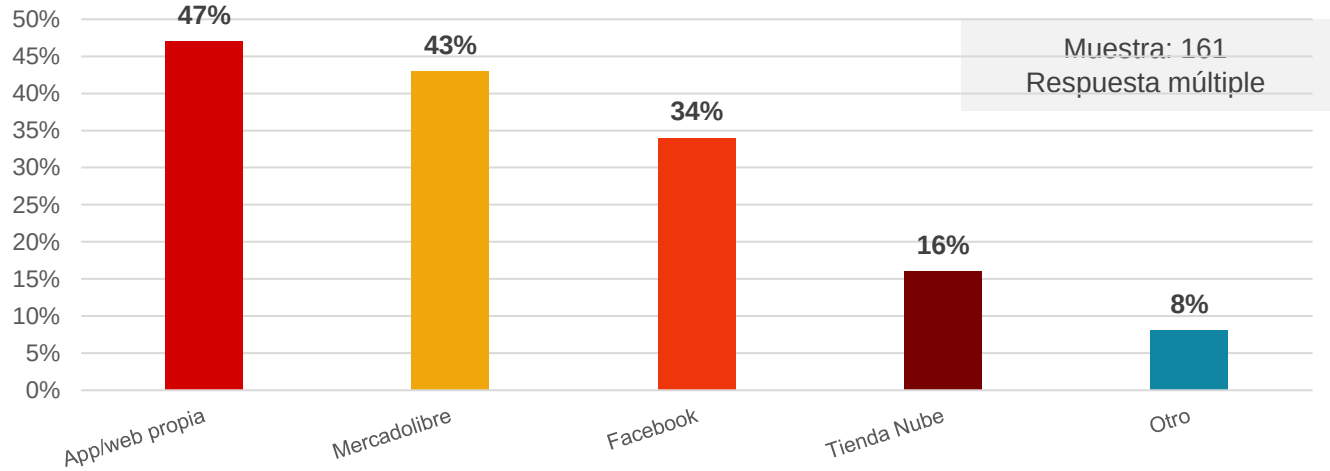
B- E-COMMERCE

¿Realizó ventas online a través de websites o apps?

Muestra: 404
Una respuesta

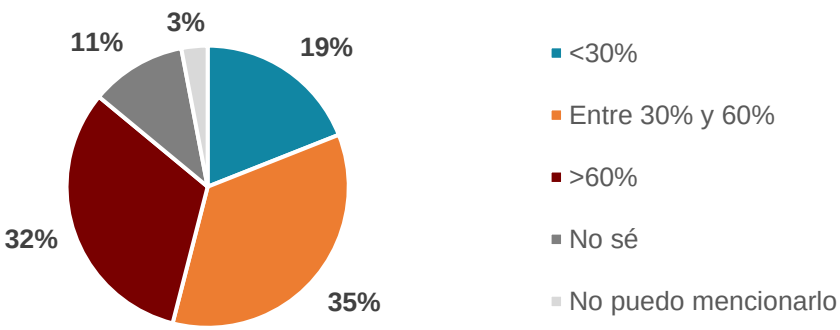


¿Realizó ventas online a través del website o app de marketplaces?



Muestra: 161
Respuesta múltiple

Porcentaje de la facturación total anual de las empresas que fue generada por la venta online de bienes o servicios

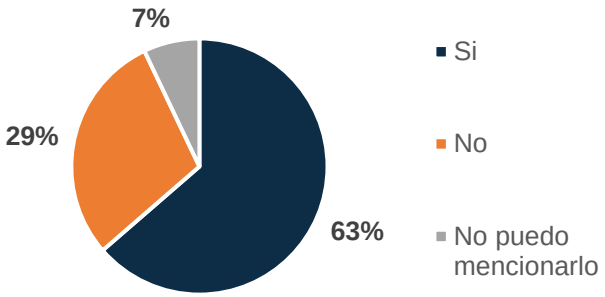


El Índice en Argentina

B- E-COMMERCE

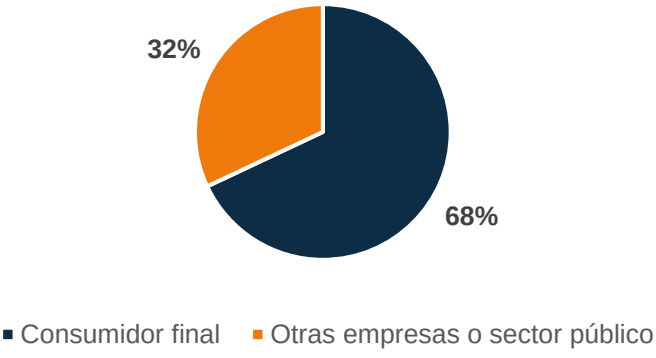
¿Más de la mitad de la facturación total en 2023 por sitios de e-commerce se concentraron en un solo sitio-plataforma?

Muestra: 161
Una respuesta



Desglose porcentual del valor de las ventas online en el último año según el tipo de consumidor.

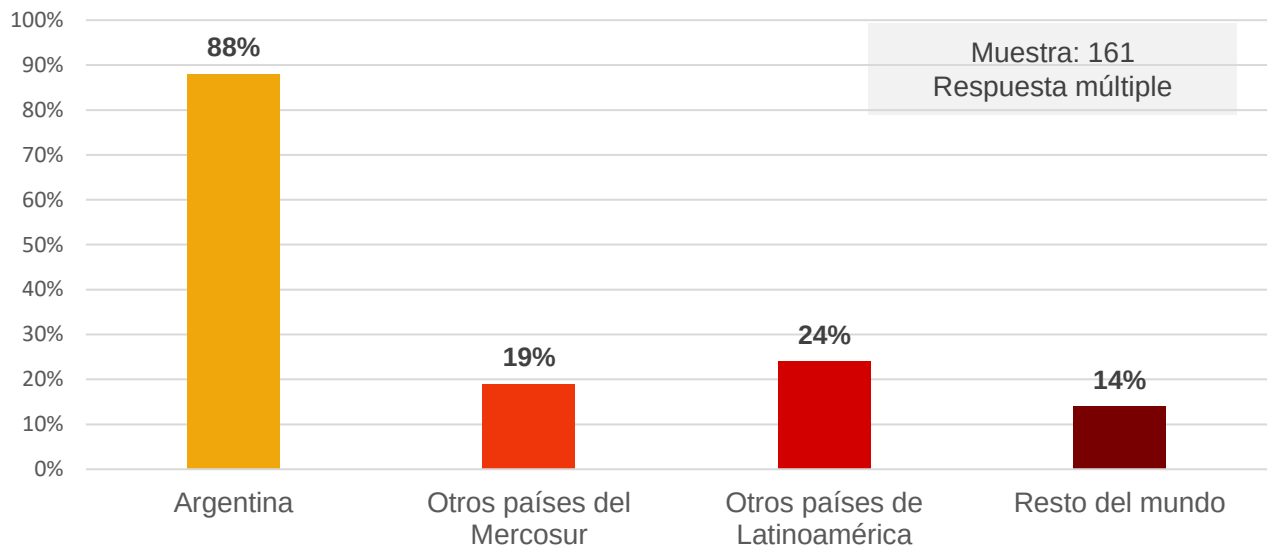
Muestra: 161
Respuesta espontánea



El Índice en Argentina

B- E-COMMERCE

Ventas online 2022/2023 a clientes situados en...



- **87,5%** facturación promedio de la venta online total anual de las empresas en 2023 que fue hacia Argentina.

- **19,2%** facturación promedio de la venta online total anual de las empresas en 2023 que fue hacia otros países del Mercosur.

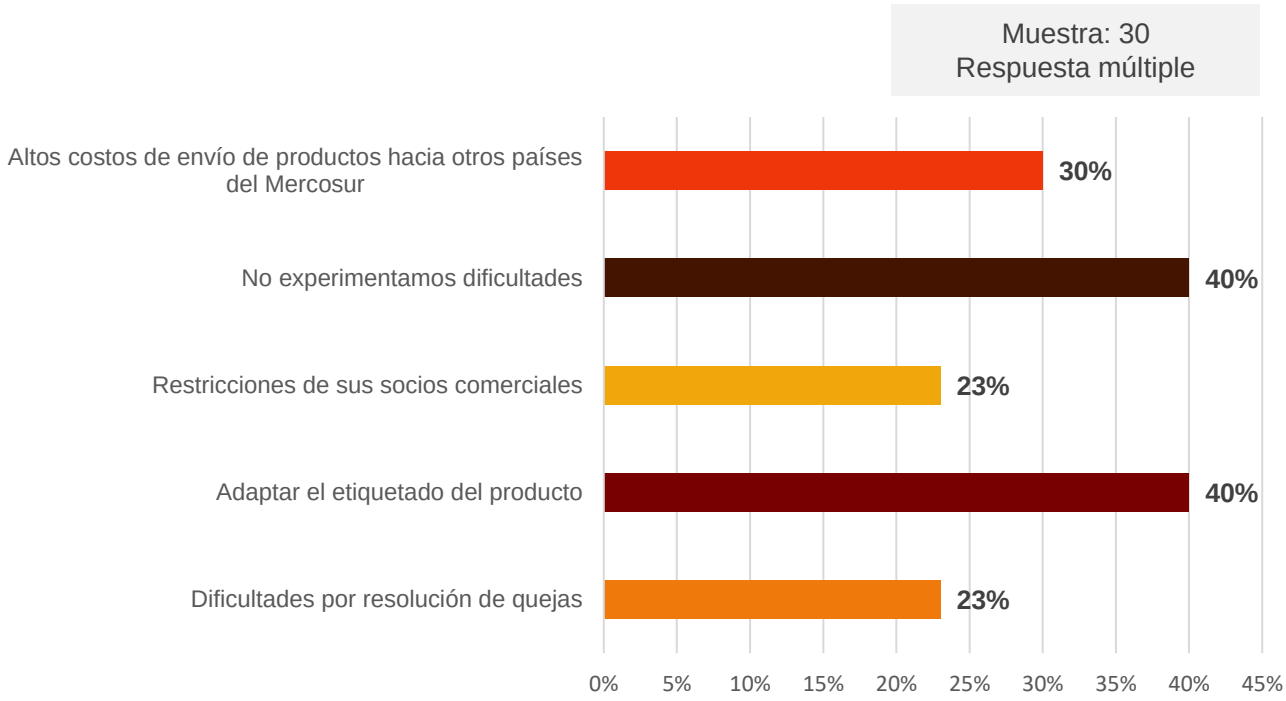
- **23,6%** facturación promedio de la venta online total anual de las empresas en 2023 que fue hacia otros países de Latinoamérica.

- **14,2%** facturación promedio de la venta online total anual de las empresas en 2023 que fue hacia otros países del resto del mundo.

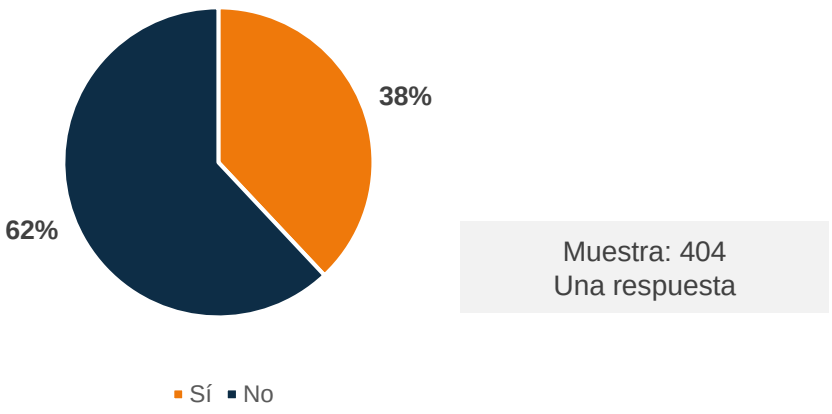
El Índice en Argentina

B- E-COMMERCE

Dificultades que experimentaron durante 2023 las empresas que destinan ventas online a otros países del Mercosur.



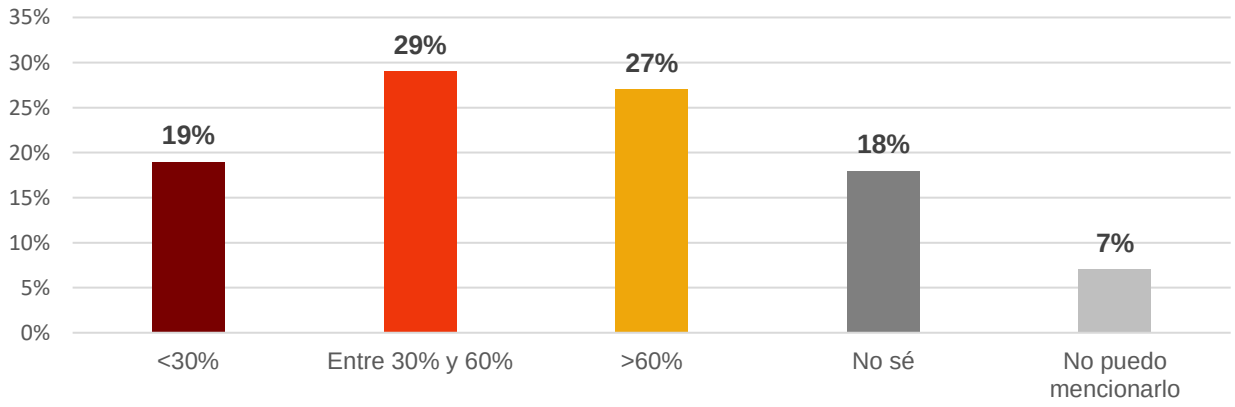
Empresas que realizaron ventas a través de procesos electrónicos (EDI-Type) durante el 2023.



El Índice en Argentina

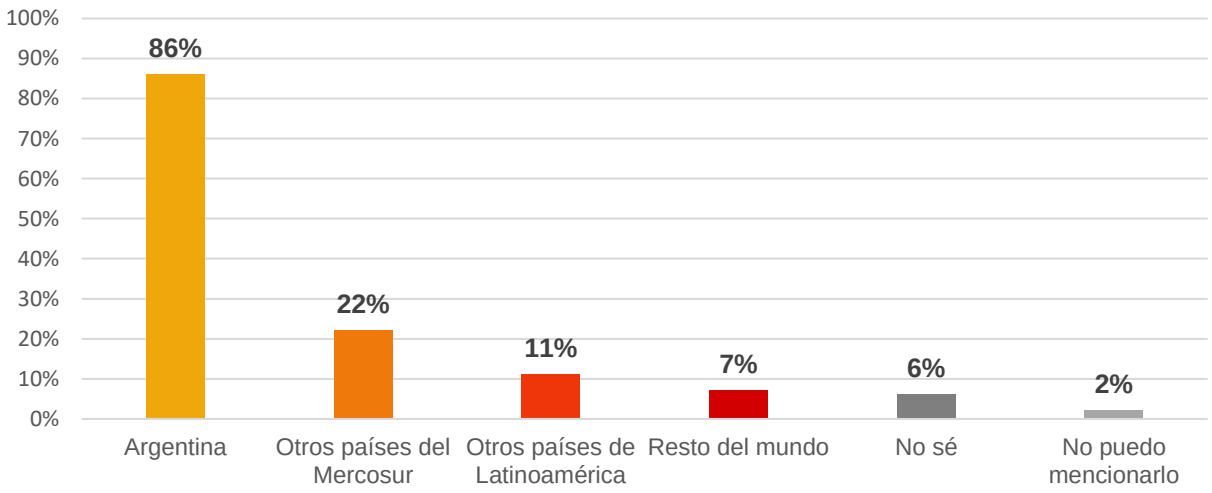
B- E-COMMERCE

Países a dónde se destinaron las ventas por procesos electrónicos (EDI-Type) durante 2023.



Muestra: 153
Respuesta múltiple

Países a dónde se destinaron las ventas por procesos electrónicos (EDI-Type) durante 2023.



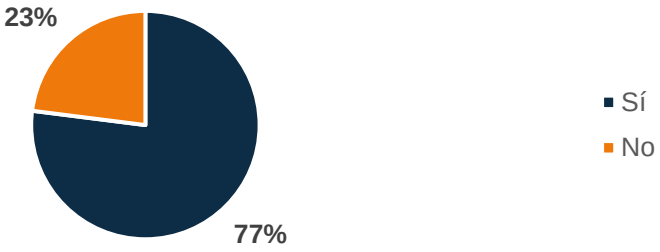
Muestra: 153
Respuesta múltiple

El Índice en Argentina

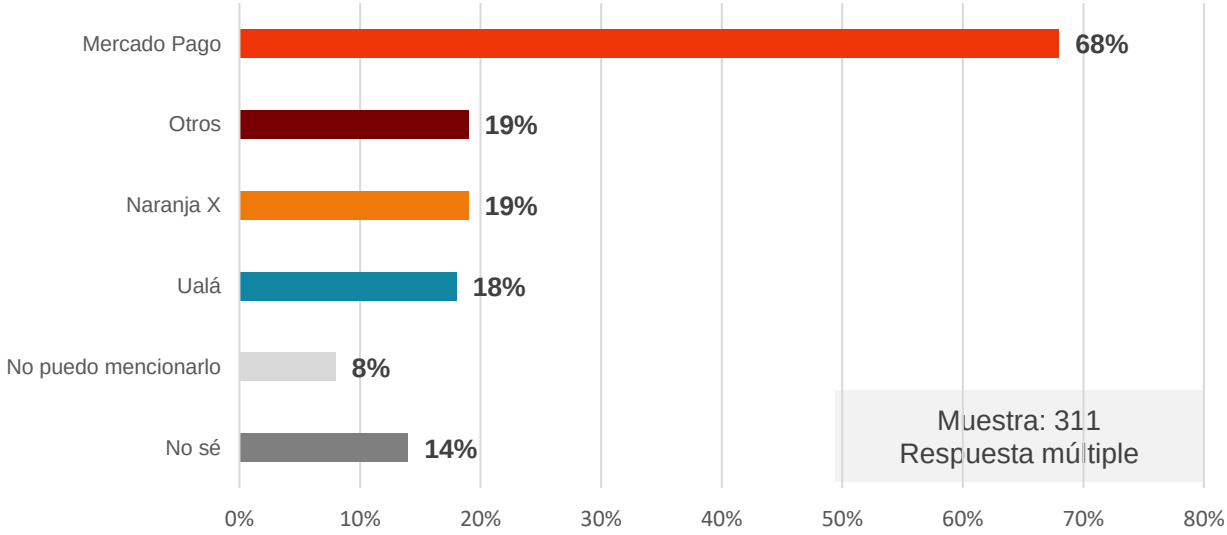
B- E-COMMERCE

Uso de medios de pago digitales.

Muestra: 404
Una respuesta

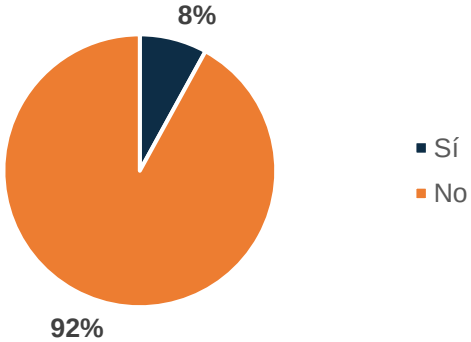


Medios de pago digitales qué más utilizan las empresas.



Empresas que utilizan criptomonedas en transacciones de cobro o pago.

Muestra: 404
Una respuesta

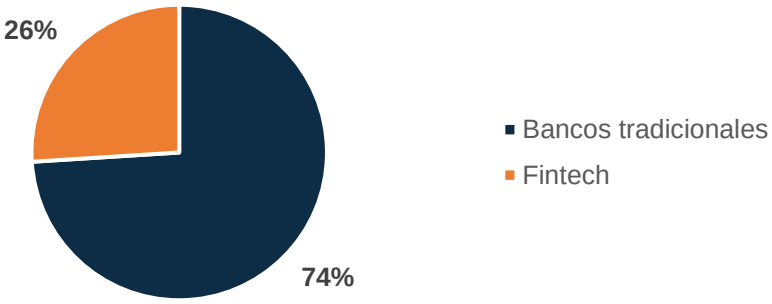


El Índice en Argentina

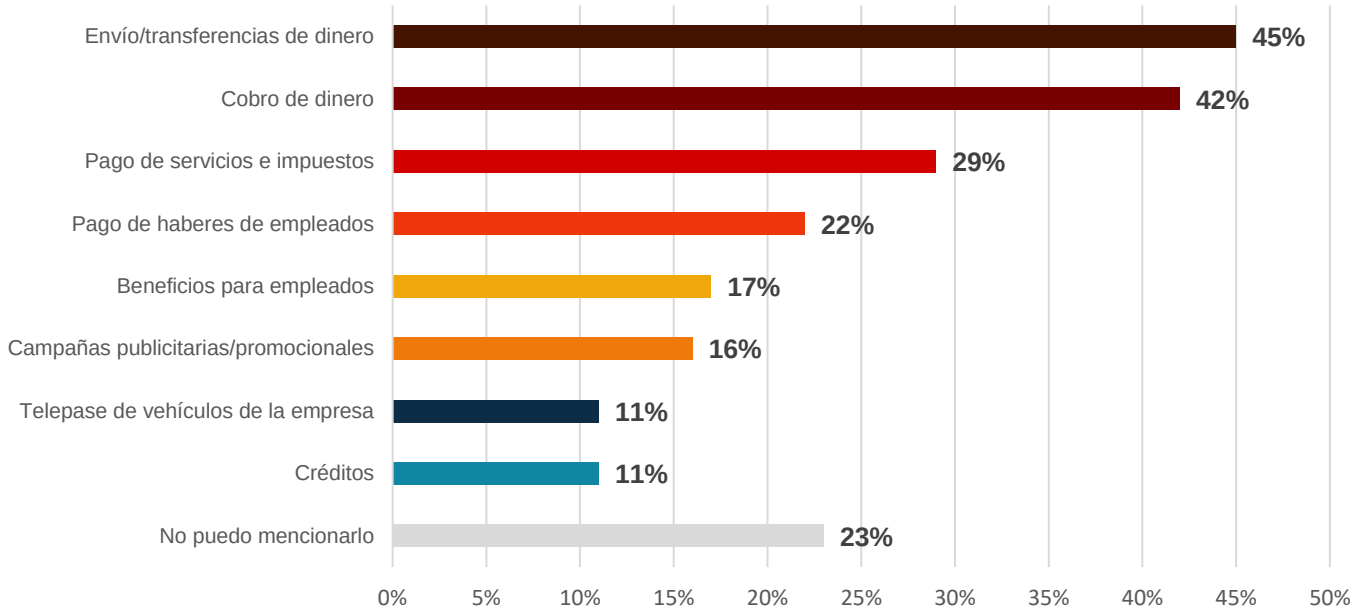
B- E-COMMERCE

Las empresas utilizan mayoritariamente servicios de bancos de tipo:

Muestra: 404
Una respuesta



Servicios de las Fintech que más utilizan las empresas.



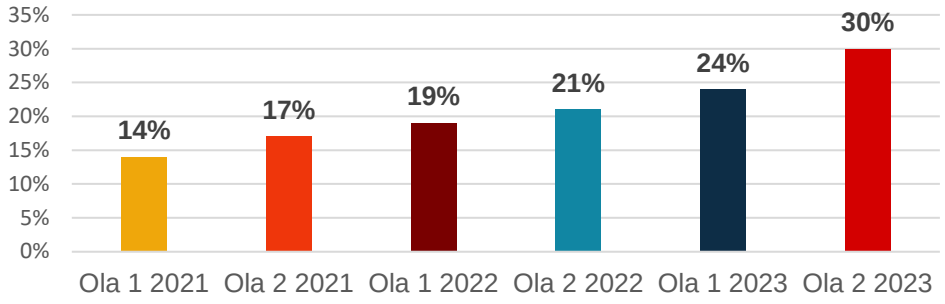
Muestra: 404
Respuesta múltiple

El Índice en Argentina

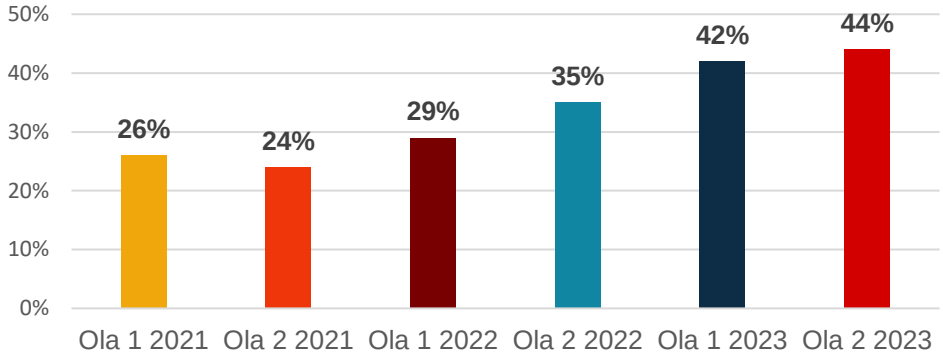
C- INTERCAMBIO DE INFORMACIÓN ELECTRÓNICAMENTE EN LA EMPRESA

Las empresas utilizan:

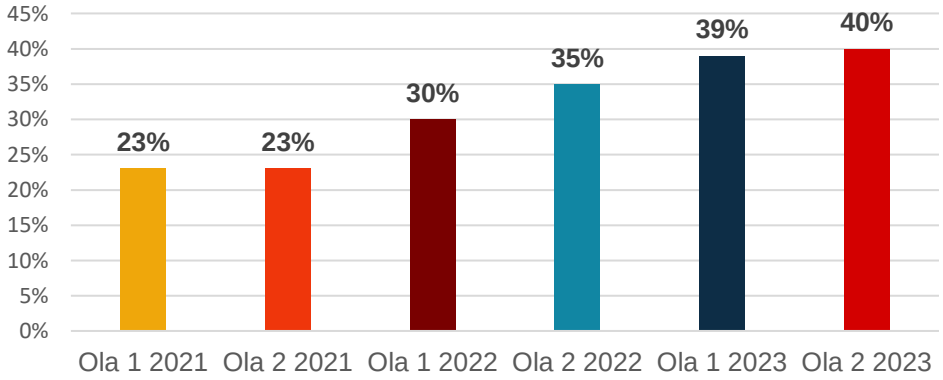
Programa de ERP: programa de gestión del negocio



CRM (gestión de relaciones con el cliente) para la recopilación de información sobre los clientes para funciones comerciales



CRM (gestión de relaciones con el cliente) para el análisis de información sobre clientes con fines de marketing

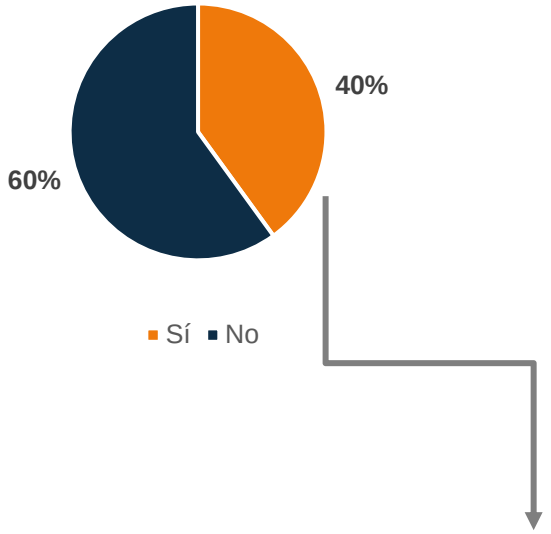


Muestra: 404
Una respuesta por opción

El Índice en Argentina

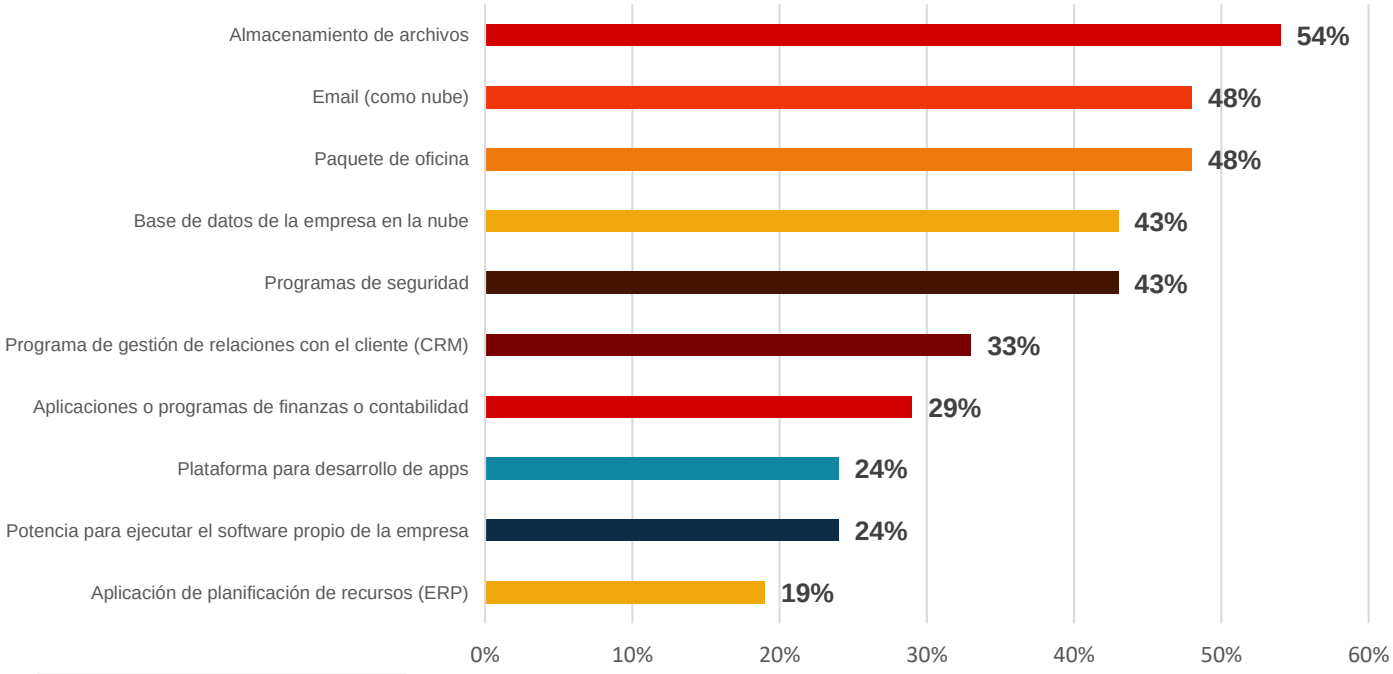
D- USO DE LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE

Empresas que compraron algún servicio de computación en la nube.



Muestra: 404
Una respuesta

Servicios de computación en la nube que utilizan las empresas.

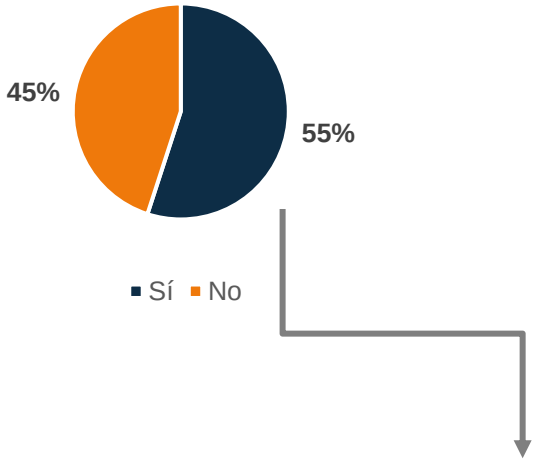


Muestra: 160
Respuesta múltiple

El Índice en Argentina

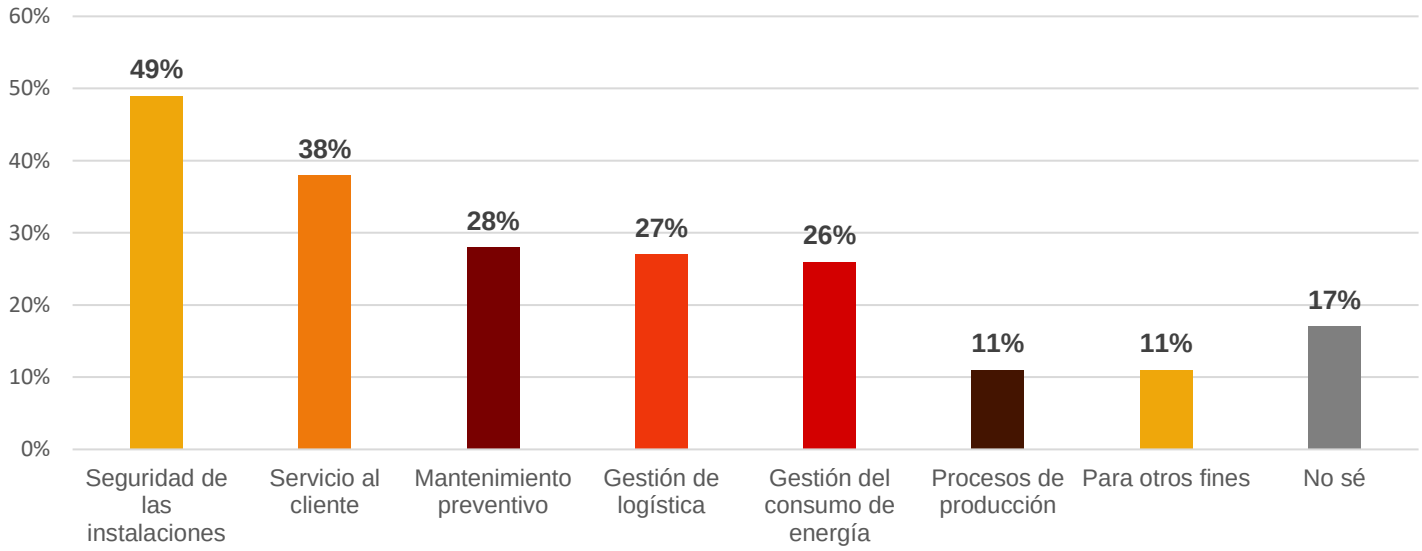
E- INTERNET DE LAS COSAS

Empresas que utilizan dispositivos o sistemas interconectados que se pueden monitorear o controlar de forma remota.



Muestra: 404
Una respuesta

Actividades para las cuales las empresas utilizan dispositivos o sistemas interconectados.

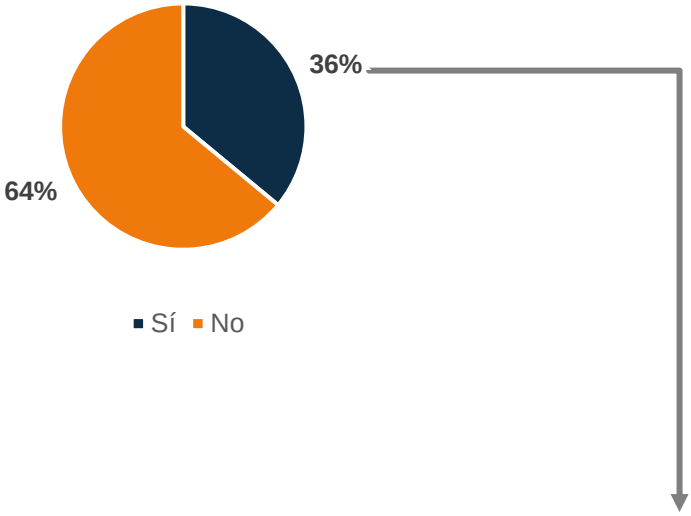


Muestra: 221
Respuesta múltiple

El Índice en Argentina

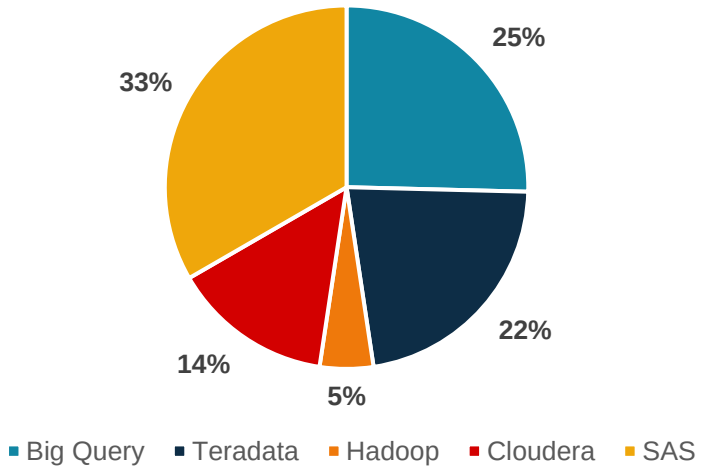
E- INTERNET DE LAS COSAS

Empresas que analizan o explotan big data internamente desde cualquier fuente de datos.



Muestra: 404
Una respuesta

Herramientas de big data que utilizan las empresas.

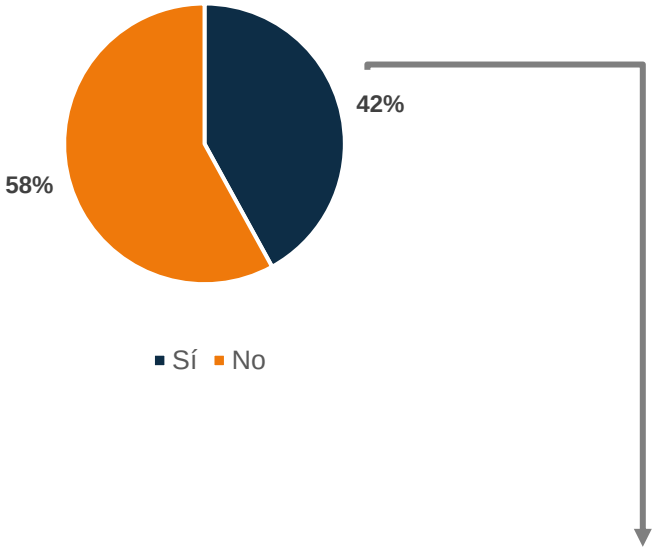


Muestra: 146
Respuesta espontánea.
Top five menciones

El Índice en Argentina

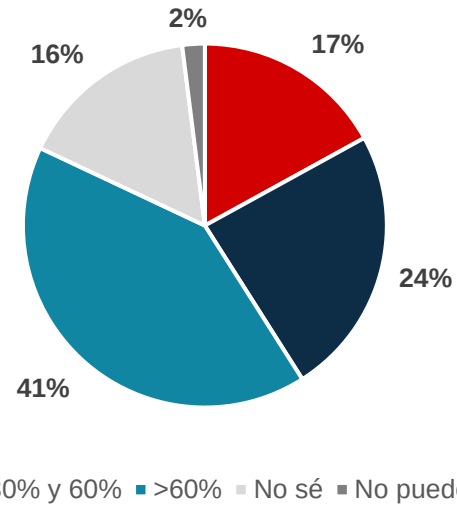
E- INTERNET DE LAS COSAS

Empresas que utilizan servicios de Call Center para soporte o atención al cliente.



Muestra: 404
Una respuesta

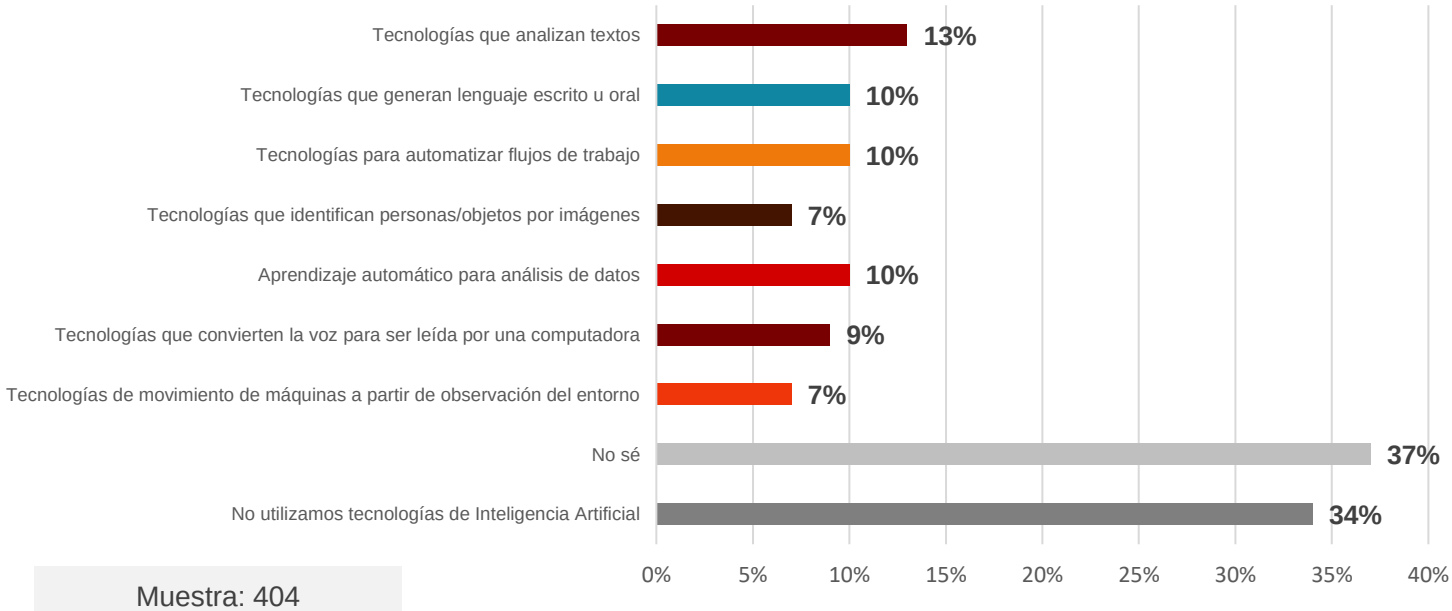
Porcentaje de reclamos de los clientes que se solucionan mediante el Call Center.



El Índice en Argentina

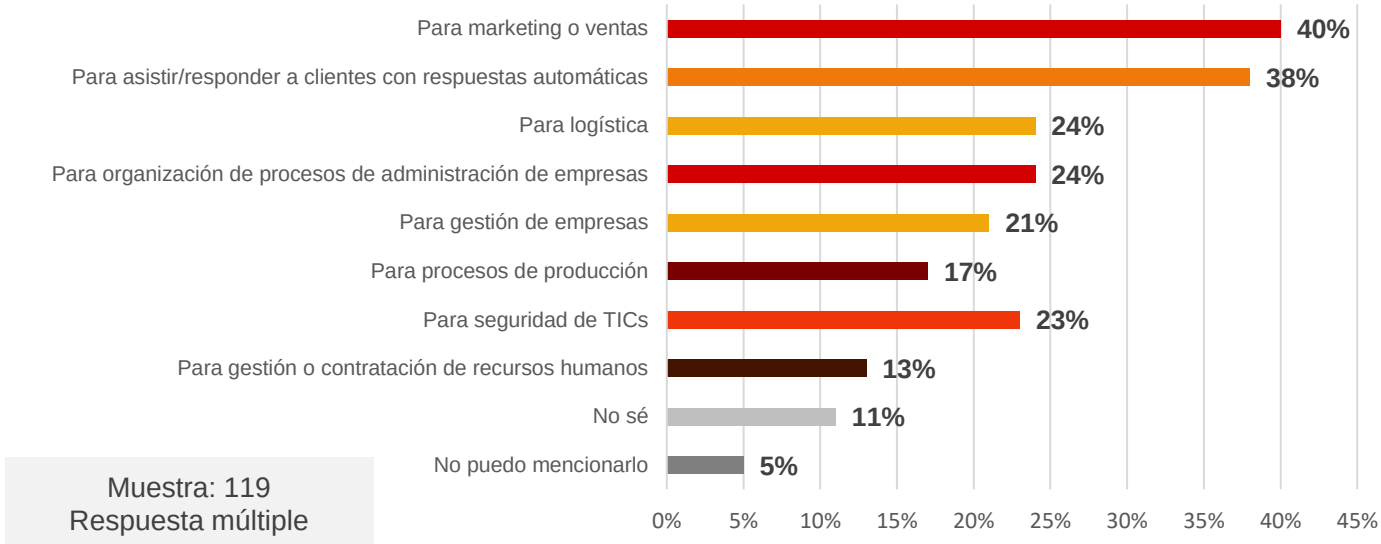
F- INTELIGENCIA ARTIFICIAL (IA)

Tecnologías-herramientas de Inteligencia Artificial (IA) que utilizan las empresas.



Muestra: 404
Respuesta múltiple

Actividades para las cuales las empresas utilizan tecnologías-herramientas de Inteligencia Artificial.

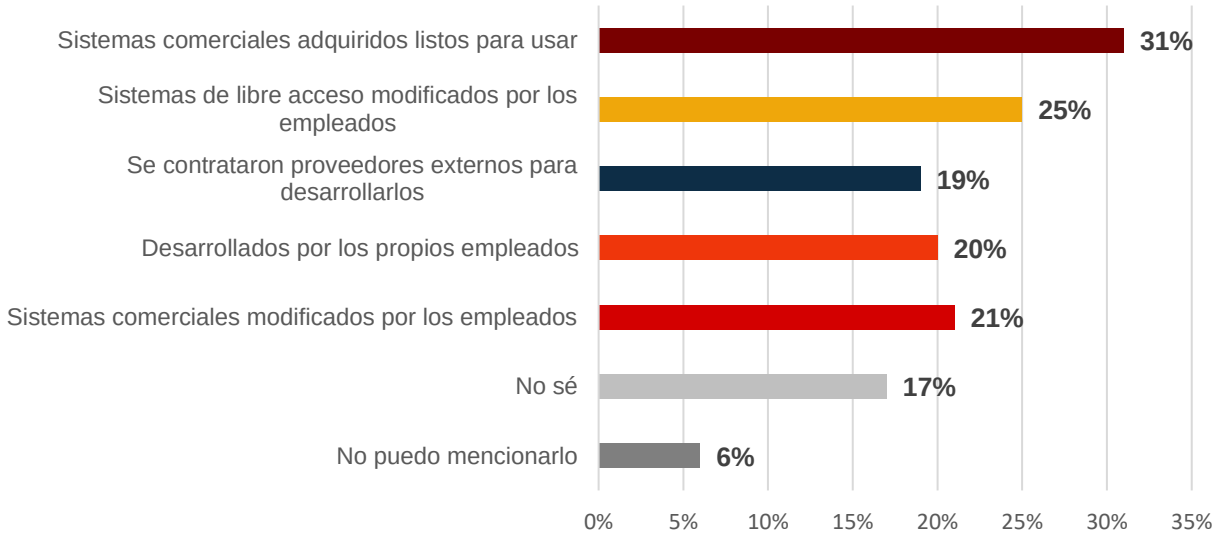


Muestra: 119
Respuesta múltiple

El Índice en Argentina

F- INTELIGENCIA ARTIFICIAL (IA)

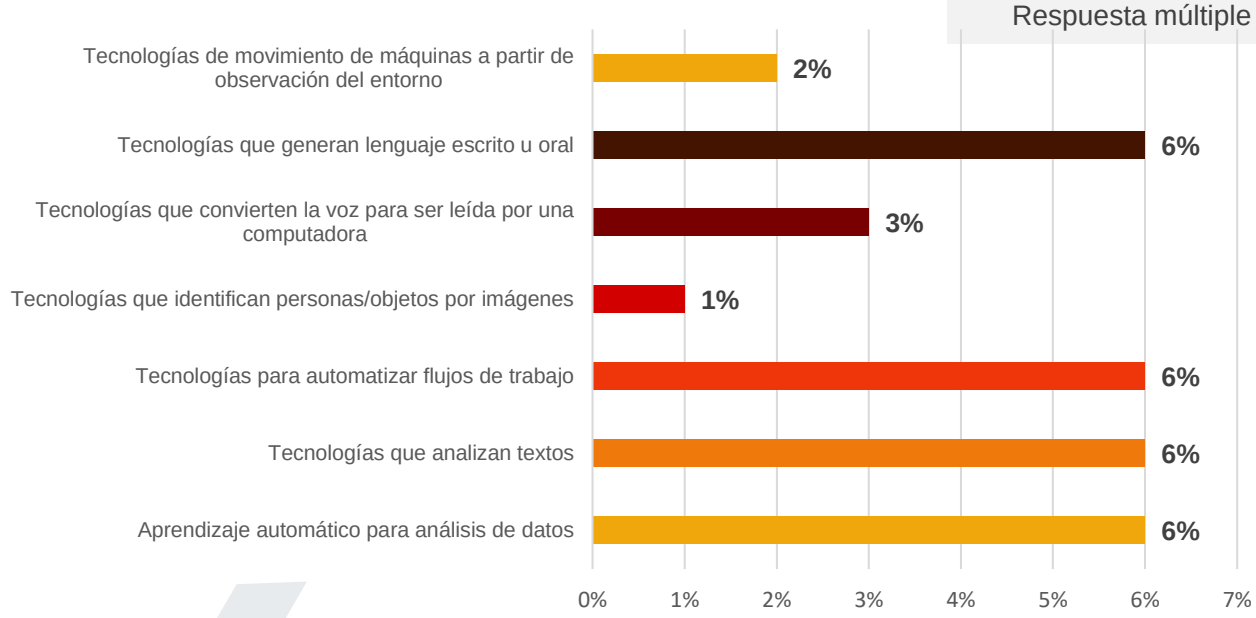
Forma de adquirencia de el/los softwares o sistemas de Inteligencia Artificial (IA) utilizados en las empresas.



Muestra: 119
Respuesta múltiple

Tecnologías-herramientas de Inteligencia Artificial que consideran utilizar las empresas.

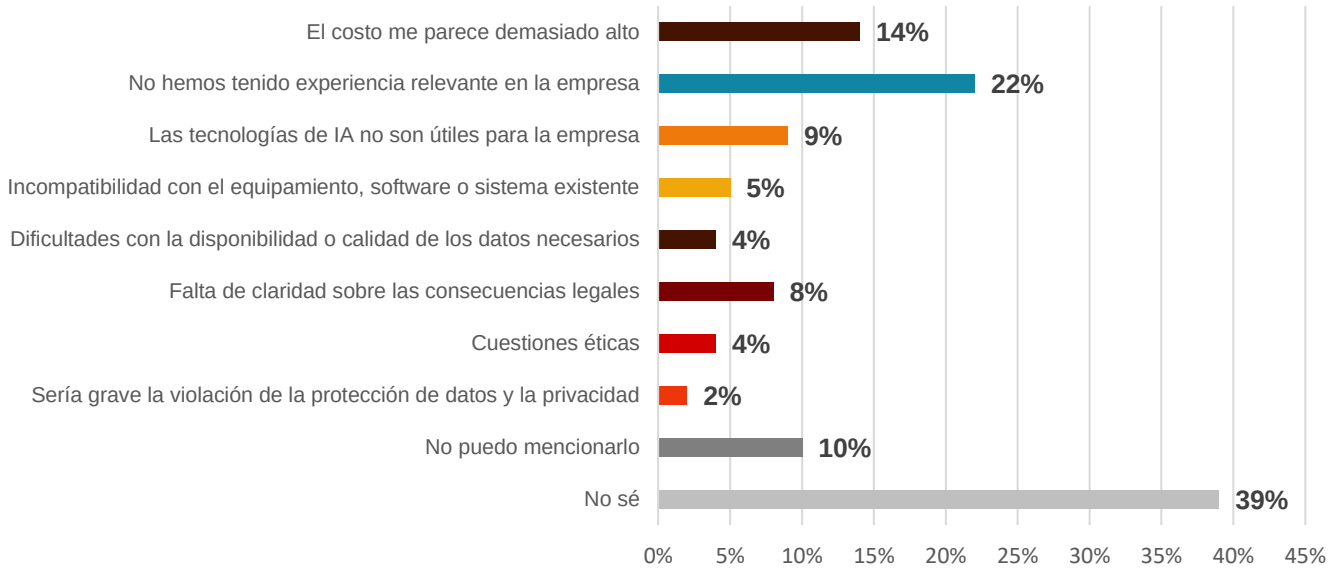
Muestra: 285
Respuesta múltiple



El Índice en Argentina

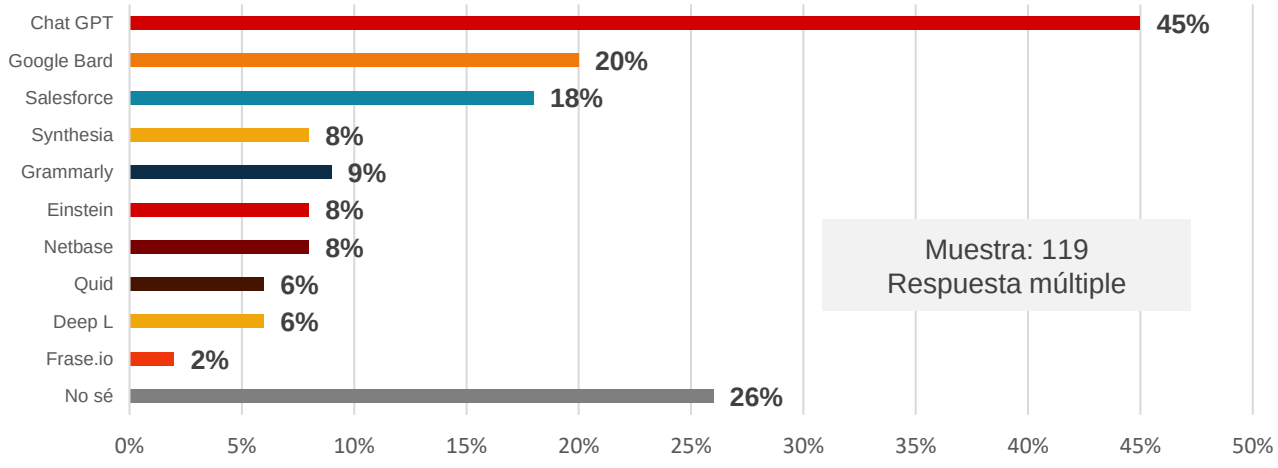
F- INTELIGENCIA ARTIFICIAL (IA)

Motivos por los que las empresas no utilizan tecnologías-herramientas de Inteligencia Artificial (IA).



Muestra: 285
Respuesta múltiple

Aplicaciones de Inteligencia Artificial (IA) que utilizan las empresas

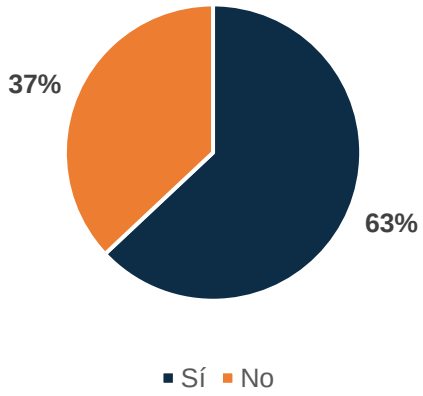


Muestra: 119
Respuesta múltiple

El Índice en Argentina

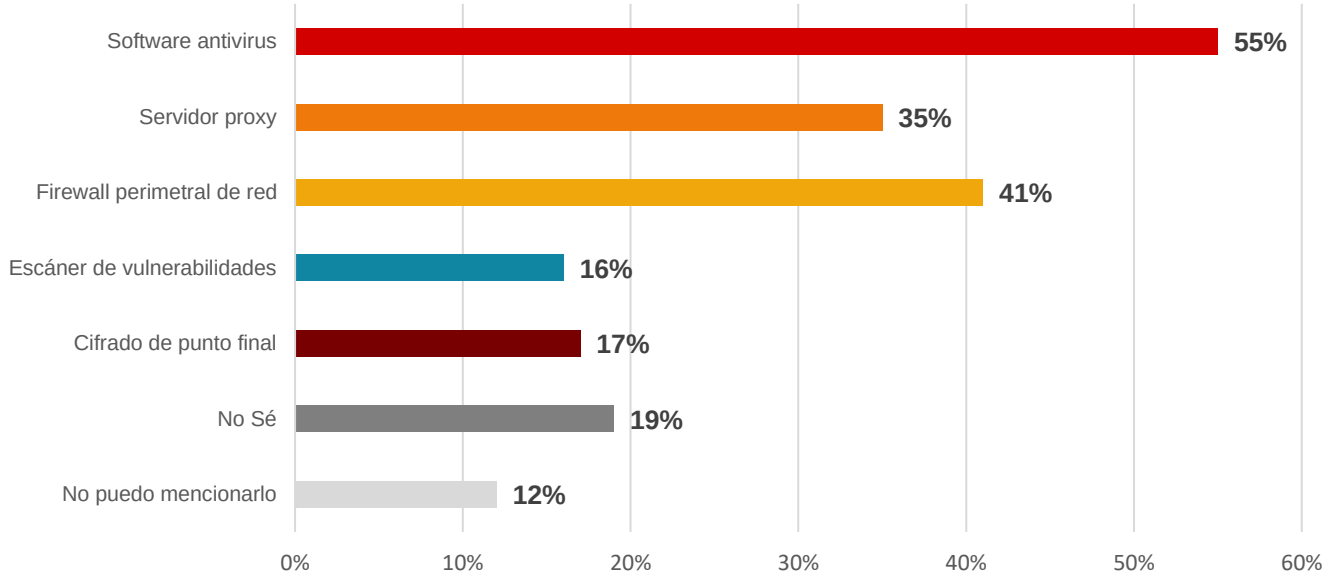
G- CIBERSEGURIDAD

Empresas que utilizan herramientas de Ciberseguridad.



Muestra: 404
Una respuesta

Herramientas de Ciberseguridad que más utilizan las empresas.

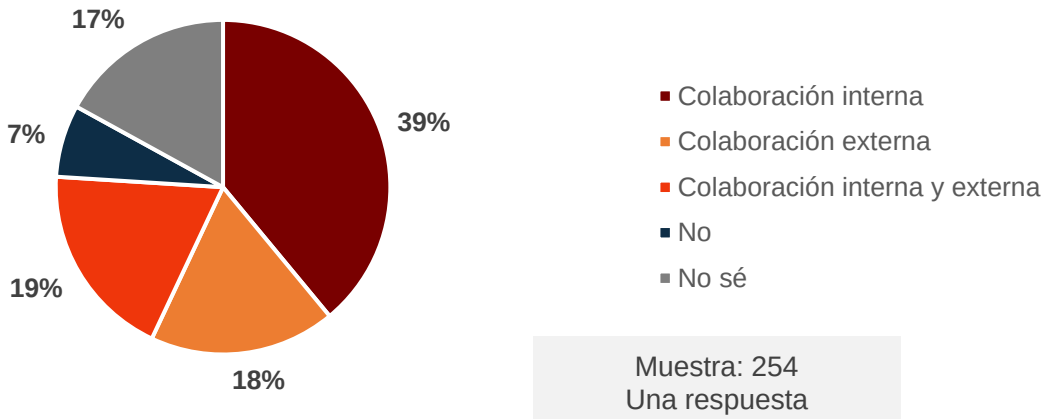


Muestra: 254
Respuesta múltiple

El Índice en Argentina

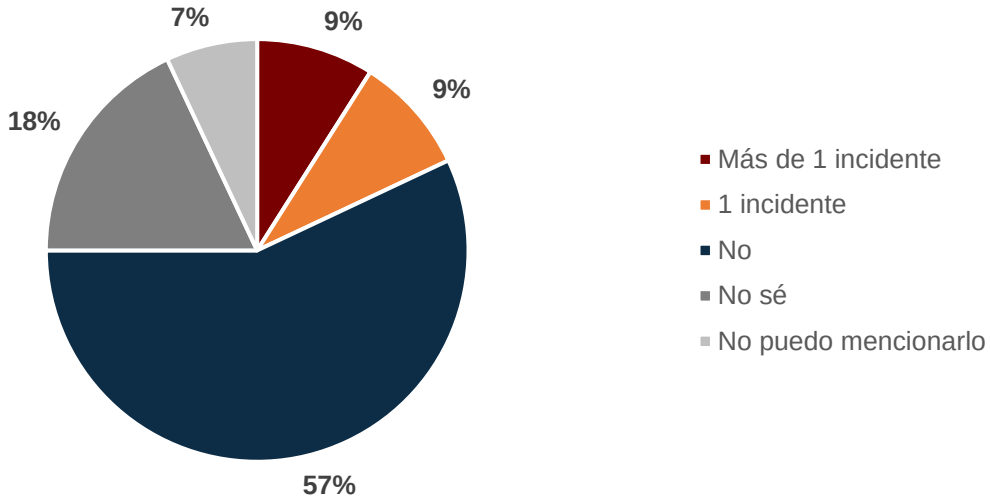
G- CIBERSEGURIDAD

Disponibilidad de al menos un colaborador interno o externo que esté especializado en Ciberseguridad.



Muestra: 254
Una respuesta

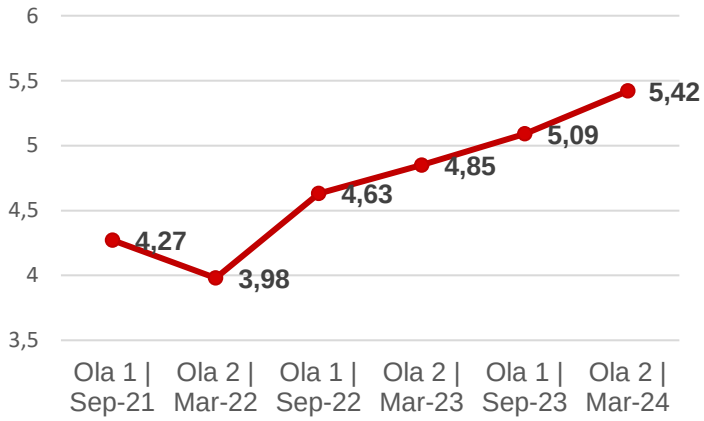
Accidentes de Ciberseguridad en el último año.



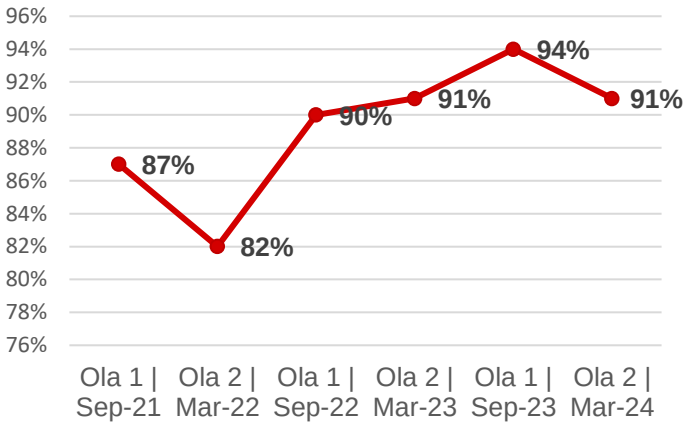
Muestra: 404
Una respuesta

Variaciones IID

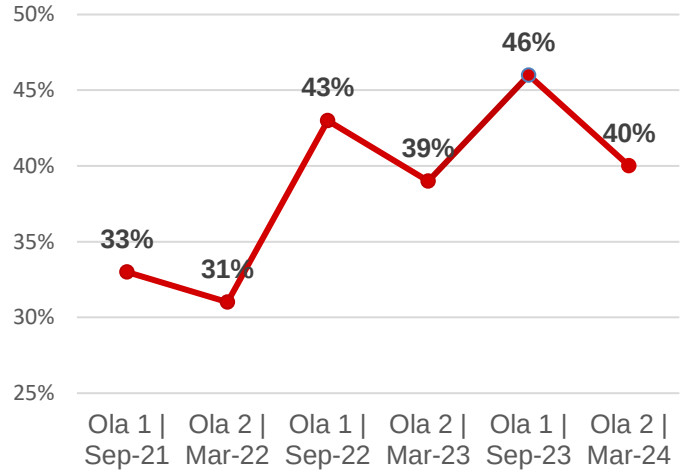
Índice de Intensidad Digital



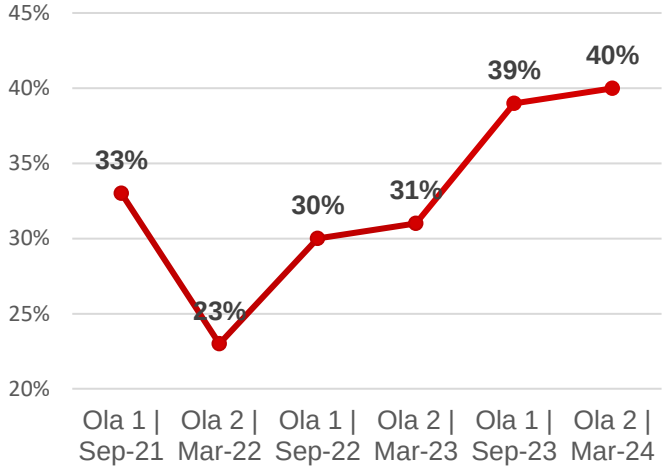
Empresas con conexión a Internet



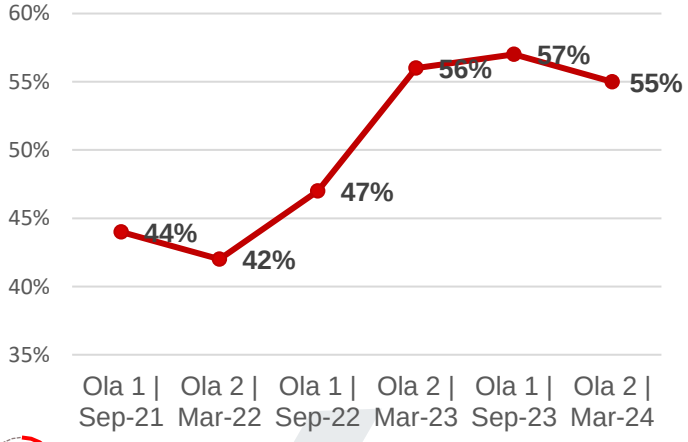
Realizaron ventas por e-commerce



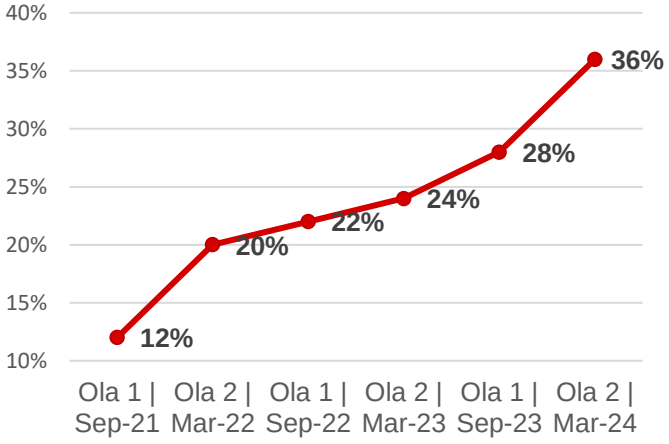
Compraron servicios en la nube



Utilizan sistemas de monitoreo en forma remota



Explotan Big Data



¿Qué pasa en el mundo?

La Comisión Europea publica todos los años su informe DESI (Digital Economy and Society Index) donde evalúa para los estados miembro de la Unión Europea algunos de los aspectos que se estudian en el Índice de Intensidad Digital (IID) en Argentina. El índice de la Economía y las Sociedades Digitales considera 33 indicadores que se agrupan en cuatro dimensiones: Conectividad, Capital Humano, Servicios públicos digitales, Integración de la tecnología digital. Si bien no todos los indicadores son comparables con el IID, tomamos los valores del último informe (2019) que se evalúan bajo los mismos criterios y desarrollamos los mismos para Chile, México y Brasil, países de nuestra región incluidos en dicho estudio. La información para Argentina se complementó con las mismas fuentes utilizadas por la UE: Banco Mundial, UNESCO y World Economic Forum (Networked Readiness Index 2019).

2da Dimensión – Capital Humano:

- % con conocimiento básico (procesador de texto)
- % con conocimiento medio (planilla de cálculo avanzada)
- % con conocimiento básico de programación
- Empleados full-time de telecomunicaciones respecto del total de empleados
- % Personas graduadas en TICs

4ta Dimensión - Integración de la tecnología digital:

- Medida de disponibilidad de las últimas tecnologías
- Inversión de las últimas tecnologías
- % Empresas (con 10 empleados o más) que reciben órdenes por internet
- Nº de servidores de internet seguros (por millón de personas)
- % que usan ecommerce
- % de ventas por ecommerce
- % ventas domesticas vs exterior

	2da dimensión	4ta dimensión
Chile	29,00%	28,60%
Brasil	35,70%	10,30%
México	34,30%	19,10%
Canada	36,50%	55,70%
EEUU	65,70%	73,40%
Argentina	43,00%	23,28%

Metodología

El Índice de Intensidad Digital (IID), mide el estado de digitalización de las empresas estudiadas. Según el número de las diferentes tecnologías y herramientas del comercio electrónico que adquieren o utilizan, las empresas escalan en el indicador.

Se realizó un estudio multisectorial de campo por la consultora OH PANEL, donde la unidad de análisis fue la empresa y el tamaño de la muestra fue de +400 observaciones entre pequeñas, medianas y grandes firmas (siendo un 80% PyMEs).

- 60% Micro y pequeñas empresas (hasta 49 empleados).
- 20% Medianas empresas (entre 50 y 200 empleados).
- 20% Grandes empresas (más de 201 empleados).

Se consideraron 13 variables cada una suma un punto en caso de disponer o utilizar la empresa dicha tecnología. La metodología utilizada determina que cada pregunta no respondida o completada sin aportar información relevante (“no sé” o “no puedo mencionarlo”) no se valora y no es tenida en cuenta para el IID. Es decir, en lugar de ser considerada como que no cumple dicho ítem, se restará del total de variables evaluadas para dicha empresa. De esta manera, cada una contará con un número que será proporcional en el caso de no haber completado los 13 ítems requeridos para la confección del índice. Esto permite comparar a las empresas entre sí, y así poder reunir toda la información para el indicador total sin que el número se vea afectado por empresas que no respondan mayormente las preguntas.

El índice de intensidad digital podrá tomar valores entre 0 y 10 siendo 0 el caso en que todas las empresas tengan un nivel nulo de digitalización y 10 en el caso de que cumplan con todas las variables (o el total sobre las que hayan respondido cada empresa encuestada). Cabe resaltar que las diferentes variables que se toman de referencia siguen los reportes elaborados por la Unión Europea cada año.