



Importancia de la ciberseguridad en las Micro, Pequeñas y Medianas empresas (MiPymes)

COORDINACIÓN GENERAL DE POLÍTICA DEL USUARIO



Introducción

Mediante un comparativo de 2019 a 2022 se desprende que las MiPymes hoy en día dan una mayor importancia al tema de ciberseguridad.¹

La presente nota tiene por objetivo mostrar el cambio en la percepción y conocimiento en materia de ciberseguridad de las MiPymes sobre la importancia, preocupaciones, medidas de seguridad implementadas al navegar en Internet, si cuentan o no con un responsable de la ciberseguridad y qué tan probable sería ser víctima de un ciberataque.

Los hallazgos mostrados sobre el cambio de percepción y conocimiento en materia de ciberseguridad de las MiPymes (2019 a 2022) cobra mayor relevancia al considerar que, **“si bien la ventaja de la tecnología digital aporta inmensos beneficios económicos y sociales, los riesgos cibernéticos pueden contrarrestar los beneficios de la digitalización”** (UIT, 2021)².

¹ Con base en las respuestas que las MiPymes han brindado a través de las Encuestas a Usuarios de Servicios de Telecomunicaciones que lleva a cabo el IFT. Los resultados de 2019 a 2022 pueden presentar variaciones que pueden ser explicadas por el error teórico de cada levantamiento.

² ITU (2021), Índice Global de Ciberseguridad. Disponible en: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/>

Contratación del servicio de Internet fijo

De 2019 a 2022, se incrementó el porcentaje de MiPymes que mencionaron contratar el servicio de Internet fijo (de 71.7% a 79.9%); por tamaño de empresa, las medianas empresas registraron el mayor crecimiento en este periodo.

Gráfico 1.

MiPymes que tienen contratado el servicio de Internet fijo (2019-2022)



◆ 2019 ◆ 2021 ◆ 2022

Nota: Debido a que se presenta únicamente el porcentaje de empresas que respondieron "Sí", la suma no da 100%.
Fuente: IFT (2023)

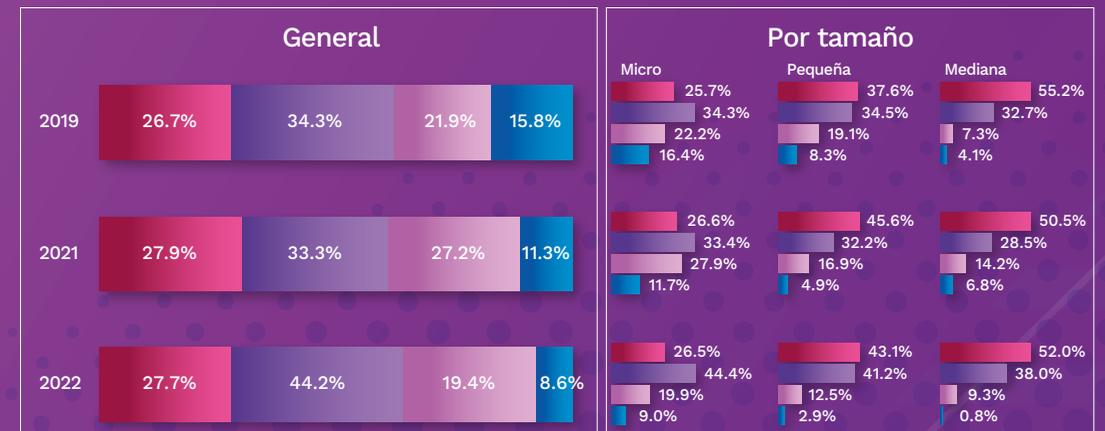
¿Qué tan importante es la ciberseguridad para las MiPymes?

En 2022, el 71.9% de las MiPymes encuestadas mencionaron que, la ciberseguridad es muy importante/importante; esta mención tuvo un incremento significativo respecto del porcentaje que registraron en 2019 (61%).

Por tamaño, la importancia de la ciberseguridad para las micro y pequeñas empresas incrementó al pasar de 60% y 72.1% en 2019 a 70.9% y 84.3% en 2022, respectivamente. En cuanto a las medianas empresas, aunque este incremento no es significativo, son las que consideran en un mayor porcentaje que la ciberseguridad es muy importante/importante.

Gráfico 2.

Importancia de la ciberseguridad para las MiPymes (2019-2022)



◆ Muy importante ◆ Importante ◆ Poco importante ◆ Nada importante

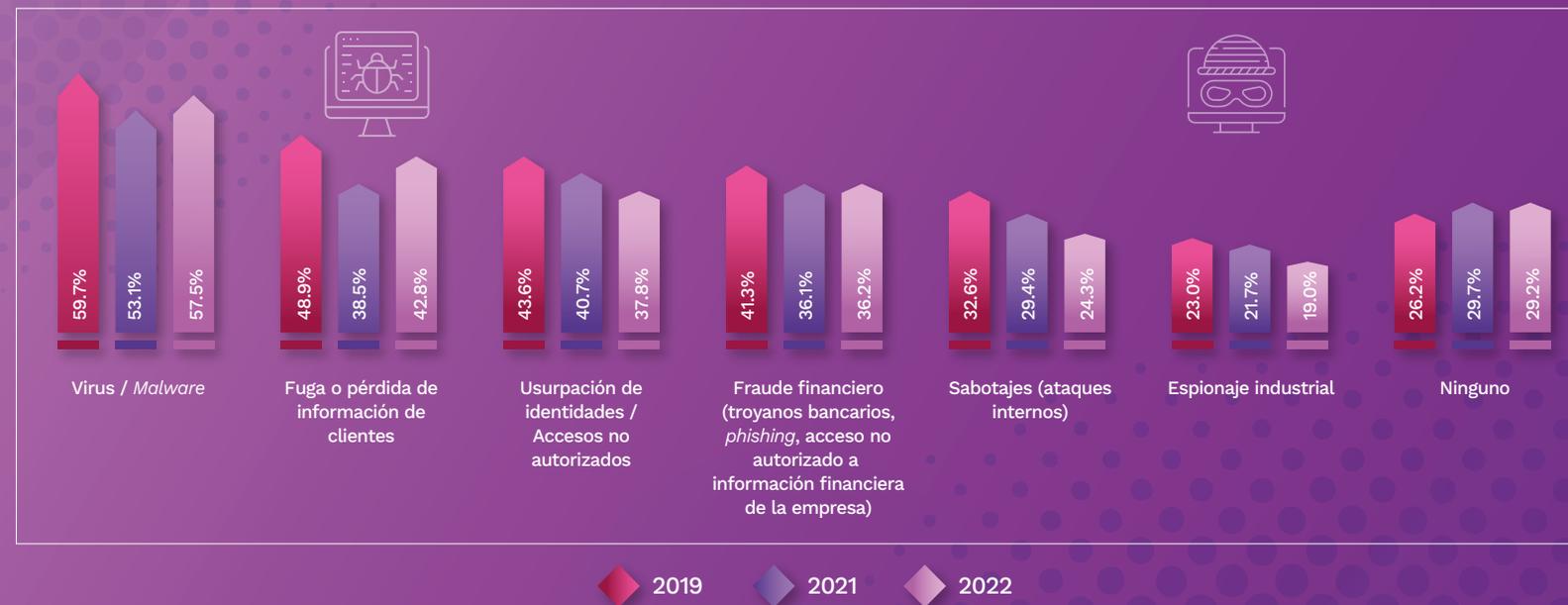
Nota: Se excluyen las menciones "No sabe/No contestó", por lo que la suma no da 100%.
Fuente: IFT (2023)

¿Cuál es la principal preocupación en caso de ser víctima de un ciberataque?

De 2019 a 2022, lo que más les preocupó a las MiPymes fue sufrir un ciberataque a través de un Virus/*Malware*; en segundo lugar, la fuga o pérdida de información de clientes y, en tercer lugar, la usurpación de identidades/accesos no autorizados.

Gráfico 3.

Preocupaciones de las MiPymes al ser víctima de un ciberataque (2019-2022)



◆ 2019 ◆ 2021 ◆ 2022

Nota: Respuesta múltiple, por lo que la suma no da 100%.
Fuente: IFT (2023)

Por tamaño, a las micro, pequeñas y medianas empresas les preocupa principalmente sufrir un ciberataque a través de un Virus/*Malware*. Es importante señalar que la preocupación de ser víctima de un ciberataque es mayor conforme aumenta el tamaño de la empresa.

Cuadro 1.

Preocupaciones de las MiPymes al ser víctima de un ciberataque, por tamaño de empresa (2019-2022)

	Micro			Pequeña			Mediana		
	2019	2021	2022	2019	2021	2022	2019	2021	2022
Virus / <i>Malware</i>	59.2%	52.1%	56.4%	64.9%	66.3%	70.8%	71.7%	67.3%	80.1%
Fuga o pérdida de información de clientes	48.3%	37.0%	41.4%	52.8%	56.9%	61.0%	73.3%	66.4%	70.8%
Usurpación de identidades / Accesos no autorizados	43.3%	39.6%	36.3%	44.3%	53.5%	55.5%	61.5%	67.5%	70.2%
Fraude financiero (troyanos bancarios, <i>phishing</i> , acceso no autorizado a información financiera de la empresa)	40.5%	35.0%	34.8%	48.0%	50.4%	53.0%	65.7%	57.7%	67.4%
Sabotajes (ataques internos)	32.2%	28.4%	23.2%	34.6%	41.7%	37.5%	50.1%	52.1%	50.2%
Espionaje industrial	22.6%	20.8%	18.2%	24.2%	32.4%	27.9%	41.6%	42.2%	45.1%
Ninguno	26.8%	30.4%	30.4%	20.2%	19.6%	14.5%	9.1%	15.5%	7.6%

Nota: Respuesta múltiple, por lo que la suma no da 100%.
Fuente: IFT (2023)

¿Qué medidas utilizan las MiPymes para resguardar la ciberseguridad de su empresa o negocio?

El antivirus fue la principal medida que las MiPymes utilizaron para resguardar su ciberseguridad, le sigue el establecimiento y cambio frecuente de contraseñas, la instalación de programas autorizados solo por el administrador de sistemas y la descarga controlada de archivos.

Gráfico 4.

Medidas que utilizan las MiPymes para resguardar la ciberseguridad (2019-2022)



◆ 2019 ◆ 2021 ◆ 2022

Nota: Respuesta múltiple, por lo que la suma no da 100%.
Fuente: IFT (2023)

El antivirus es la principal medida que las micro, pequeñas y medianas empresas han implementado para resguardar su ciberseguridad.

Asimismo, de 2019 a 2022 incrementó la implementación de otras medidas de seguridad en las pequeñas y medianas empresas como el establecimiento y cambio frecuente de contraseñas, el acceso restringido a páginas web, la capacitación o concientización del personal, etc.

Finalmente, es importante señalar que el uso de medidas para resguardar la ciberseguridad es mayor conforme aumenta el tamaño de la empresa.

Cuadro 2.

Medidas que utilizan las MiPymes para resguardar la ciberseguridad, por tamaño de empresa (2019-2022)

	Micro			Pequeña			Mediana		
	2019	2021	2022	2019	2021	2022	2019	2021	2022
Antivirus	73.4%	69.5%	70.7%	79.7%	85.5%	83.7%	88.9%	88.8%	91.4%
Establecimiento y cambio frecuente de contraseñas	60.3%	50.9%	57.5%	67.1%	68.4%	74.2%	79.0%	75.6%	85.1%
Instalación de programas autorizados solo por el "Administrador"	60.5%	53.4%	55.6%	74.0%	77.2%	71.6%	79.0%	83.2%	86.1%
Descarga controlada de archivos	60.2%	52.6%	54.9%	63.6%	73.3%	72.4%	81.8%	79.5%	81.9%
Acceso restringido a páginas web	55.4%	47.9%	54.3%	63.7%	68.4%	75.4%	80.0%	73.1%	84.6%
Acceso de información a empleados específicos	53.3%	44.5%	47.4%	64.2%	69.4%	75.9%	75.8%	78.3%	81.0%
Políticas de uso de correos electrónicos	49.4%	43.7%	45.6%	61.4%	66.4%	66.5%	73.5%	72.5%	77.7%
Capacitación o concientización del personal	42.9%	39.8%	41.2%	54.6%	66.9%	64.7%	74.0%	71.9%	80.4%
Ninguno	12.4%	14.2%	15.2%	6.3%	5.9%	6.0%	2.5%	7.7%	0.8%

Nota: Respuesta múltiple, por lo que la suma no da 100%.
Fuente: IFT (2023)

Asimismo, de los resultados obtenidos en el estudio cualitativo a MiPymes, se desprende que estas empresas reconocen el incremento de fraudes cibernéticos, por ello mantienen hábitos seguros como el cambio de contraseñas, no abren correos maliciosos, han brindado capacitaciones sobre el tema a sus empleados, recomiendan no conectarse a redes públicas cuando están en *home office*, tienen cifrado especial para las computadoras de la empresa y si surge algún problema tienen indicaciones de a quién contactar.

Diagrama 1.

Medidas de ciberseguridad de las MiPymes participantes del estudio cualitativo



Consideran que, debido a la pandemia, el comercio electrónico tuvo un incremento y con él, un incremento en los fraudes cibernéticos.



Algunos mencionaron que tienen hábitos seguros (cambio de contraseñas y revisar la dirección [https//](https://), entre las mencionadas) de uso de las plataformas y que no necesitan instalar un antivirus.

Además



- Varios han recibido capacitaciones en el tema de la ciberseguridad por parte de sus empresas. Les informan de los tipos de amenazas y los canales de denuncia.
- Les dan recomendaciones para el *home office*, como no conectarse a redes públicas, y les dan cifrado especial para sus computadoras de la empresa. Así como no abrir correos maliciosos y detectar correos falsos.
- Si surgiera algún problema, tienen instruido ir directamente con el encargado de sistemas. Las acciones que hacen es el bloqueo de usuarios y avisan a todo el personal sobre correos maliciosos.

“En mi caso, nunca hemos sufrido un ciberataque, pero cuando trabajamos en casa nos hicieron recomendaciones muy similares a nosotros sobre la red interna que tuvieron que aperturarla, no abrirla en equipos ajenos a los de la empresa porque la mayoría tenemos laptop, se facilitó para poderla tener en nuestro domicilio y el antivirus de la empresa tenerlo siempre habilitado.”

Empresas medianas



Nota: Información correspondiente al estudio cualitativo y no es representativo a nivel nacional.
Fuente: IFT (2023)

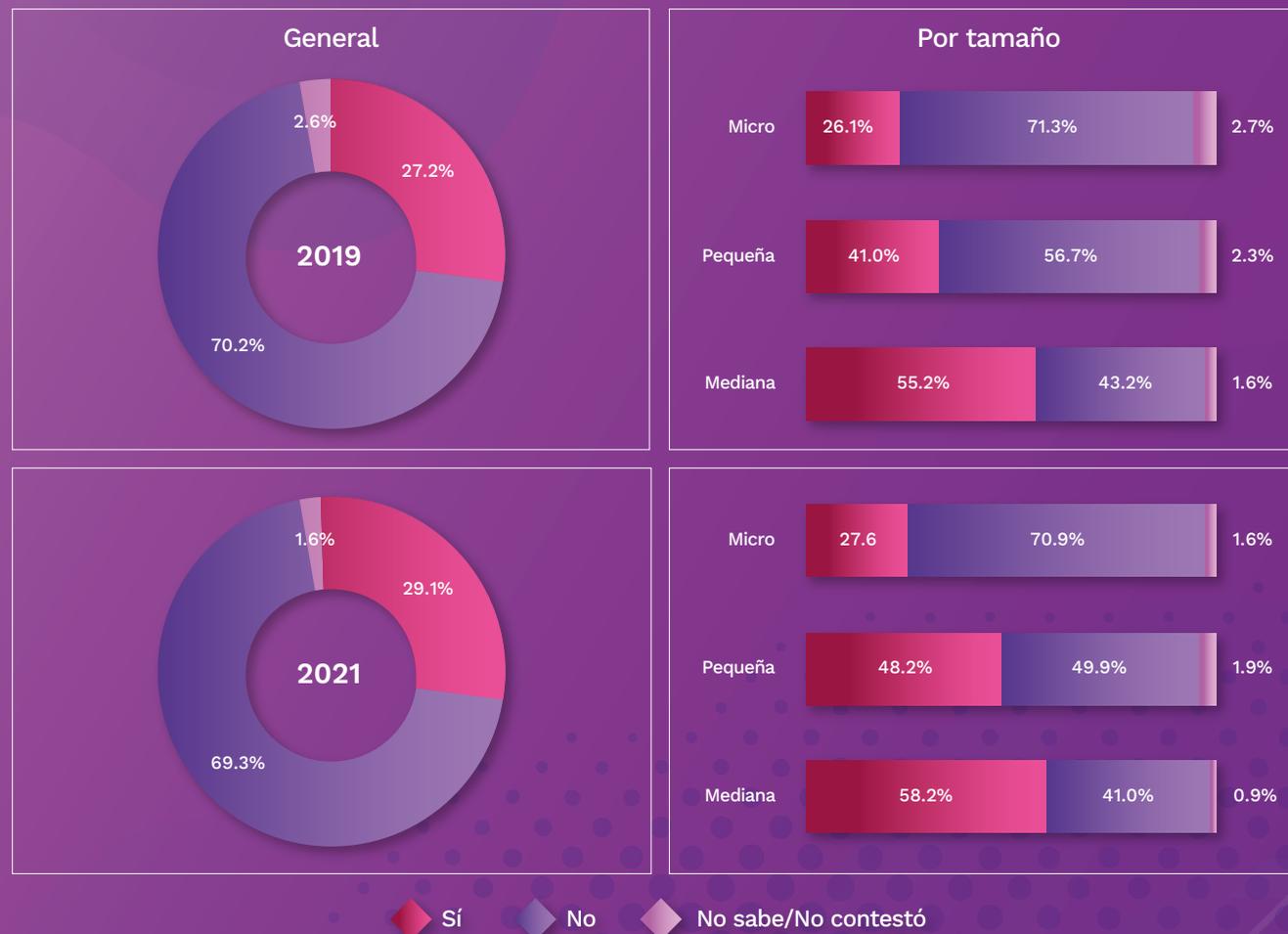
¿En la empresa o negocio hay un responsable de la ciberseguridad?

En general, aumentaron las MiPymes que mencionaron contar con un responsable de la ciberseguridad de su empresa, al pasar de 27.2% en 2019 a 29.1% en 2021.

Por tamaño, en 2021 el 58.2% de las medianas empresas mencionaron contar con un responsable de la ciberseguridad, le siguen las pequeñas empresas con 48.2% y las microempresas con 27.6%.

Gráfico 5.

¿En la empresa o negocio hay un responsable de la ciberseguridad? (2019-2021)



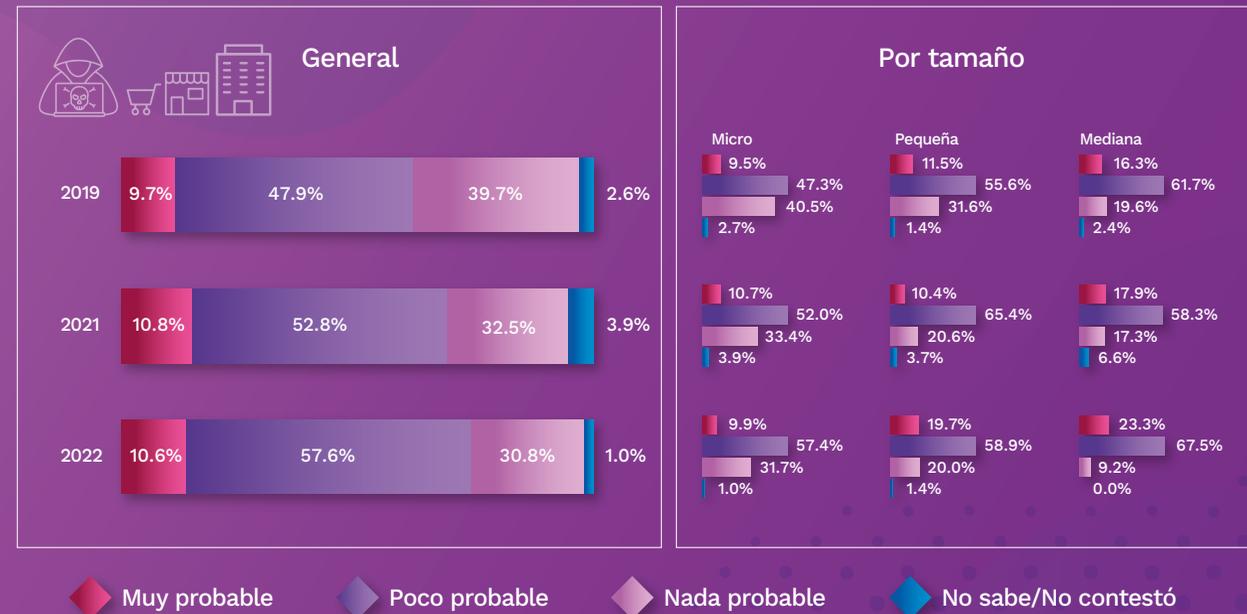
Nota: Debido al redondeo de cifras, la suma no da 100%. La pregunta no se aplicó en el año 2022.
Fuente: IFT (2023)

¿Qué tan probable cree que su empresa o negocio pueda ser víctima de un ciberataque?

De 2019 a 2022, la mayoría de las MiPymes mencionaron que es poco probable ser víctimas de un ciberataque. Por tamaño, las microempresas creen en menor medida que pueden llegar a ser víctimas de algún ciberataque en comparación con las pequeñas y medianas empresas.

Gráfico 6.

¿Qué tan probable cree que su empresa o negocio pueda ser víctima de un ciberataque? (2019-2022)



Nota: Debido al redondeo de cifras, la suma no da 100%.
Fuente: IFT (2023)

Aunado a lo anterior, las MiPymes mencionan que es más difícil que una empresa sufra algún ciberataque debido a que perciben que los sistemas y servicios empresariales tienen mayor seguridad, sin embargo, no las exentan de sufrir algún ciberataque.

Diagrama 2.

¿Han sufrido algún ciberataque las MiPymes participantes del estudio cualitativo?

La mayoría nunca ha sufrido un ciberataque y no consideran enfrentarse a algún reto con respecto a la ciberseguridad de sus dispositivos y cuentas.



Consideran que es más fácil y común que una persona física sufra un ciberataque, pero no así una empresa, pues perciben mayor seguridad en los sistemas y servicios empresariales.

“Se dio mucho y hasta la fecha se han dado mucho el caso de que llega algún correo al equipo de finanzas por ejemplo timbrado como una factura y lo abren, ahí caemos en alguna descarga de virus o cualquier robo de datos. También nos tocaba que al director general le llegaban correos de proveedores o supuestos proveedores de productos/servicios por algún reclamo cuando eran falsos, inmediatamente se recurría al área para hacer los reportes oportunos y avisar a todos, sabemos que tenemos muchos compañeros, a veces la tecnología no es lo suyo y confían tanto. Cualquier archivo que confían otras personas, confiamos un poquito más y ahí es donde caemos, se le puede infectar el equipo y tiene mucha información sensible.”

Empresas medianas



Nota: Información correspondiente al estudio cualitativo y no es representativo a nivel nacional.
Fuente: IFT (2023)

Consideraciones Metodológicas Encuestas a Usuarios de Servicios de Telecomunicaciones³

Tamaño de la muestra:

2019: 1,582 entrevistas efectivas

Distribución:

- Microempresas 1,128 entrevistas,
- Pequeñas empresas 304 entrevistas, y
- Medianas empresas 150 entrevistas.

2021: 1,601 entrevistas efectivas

Distribución:

- Microempresas 1,128 entrevistas,
- Pequeñas empresas 323 entrevistas, y
- Medianas empresas 150 entrevistas.

2022: 1,908 entrevistas efectivas

Distribución:

- Microempresas 1,360 entrevistas,
- Pequeñas empresas 366 entrevistas, y
- Medianas empresas 182 entrevistas.

Nivel de confianza y margen de error:

2019: A un nivel de confianza del 95%, se cuenta con un error absoluto teórico aproximado de **2.46%** para el total nacional.

2021: A un nivel de confianza del 95%, se cuenta con un error absoluto teórico aproximado de **2.5%** para el total nacional.

2022: A un nivel de confianza del 95%, se cuenta con un error absoluto teórico aproximado de **2.25%** para el total nacional.

Informante:

Dueños, socios, responsables, directores y/o personal que tuvieran conocimiento acerca de los servicios de telecomunicaciones (Internet fijo y/o Telefonía fija) en la empresa o negocio.

Representatividad:

Nacional

Periodos de levantamiento:

2019: Del 3 al 24 de septiembre de 2019.

2021: Del 5 de junio al 7 de agosto de 2021.

2022: Del 9 de junio al 8 de agosto de 2022.

Público Objetivo:

La muestra del estudio comprende a las MiPymes usuarias de los servicios de Internet fijo y/o Telefonía fija conforme a la siguiente segmentación:

- Micro: hasta 10 personas
- Pequeña: de 11 a 50 personas
- Mediana: de 51 a 250 personas

Levantamiento muestral:

Levantamiento presencial en unidades económicas fijas (excluyendo semifijas) con un diseño muestral probabilístico polietápico con base en el Directorio Estadístico Nacional de Unidades Económicas (DENUE) del INEGI.

Marco muestral:

La muestra está conformada por los sectores económicos más representativos utilizando el Sistema de Clasificación Industrial de América del Norte 2018 (SCIAN 2018) de INEGI; excluyendo los sectores 11, 21, 22 y 93, debido a que estos sectores en conjunto representan alrededor del 1% del total de unidades económicas fijas.

Nota: Debido a que el objetivo no es medir la penetración de los servicios, el público objetivo consistió en usuarios de Internet fijo y/o Telefonía fija y, en caso de que la unidad económica no fuera usuaria de alguno de estos dos servicios, no se entrevistó. Asimismo, el estudio se enfocó en esos dos servicios debido a que son los de mayor adopción en México.

³ Para mayor información puede consultar:
<https://www.ift.org.mx/usuarios-y-audiencias/encuestas-trimestrales>

Consideraciones Metodológicas del estudio cualitativo

Esta nota presenta información de los resultados de las sesiones de los **Focus Group**⁴ con micro, pequeñas y medianas empresas (MiPymes) que se realizaron vía *online*⁵ a través de la plataforma Teams, con la finalidad de analizar a profundidad la información que sea de relevancia para la investigación.

Para ello, se realizaron dos grupos focales los días **30 y 31 de agosto de 2022**, cada uno con una duración aproximada de 120 minutos con 6 participantes en cada sesión.



Nota: Es importante señalar que los resultados y/o aseveraciones presentadas en los estudios cualitativos no son extrapolables al total de la población; es decir, no son representativos a nivel nacional. Asimismo, estos resultados corresponden a las experiencias, opiniones y sugerencias que las personas que participaron emitieron durante el estudio cualitativo, lo anterior con la finalidad de que la persona lectora tome la información con la salvedad correspondiente.

⁴ El *Focus Group* es una técnica que centra su atención en la pluralidad de respuestas obtenidas de un grupo de personas, y es definida como una técnica de la investigación cualitativa cuyo objetivo es la obtención de datos por medio de la percepción, los sentimientos, las actitudes y las opiniones de grupos de personas.

⁵ Derivado de la contingencia ocasionada por la pandemia de coronavirus (COVID-19), los *Focus Group* se realizaron bajo la modalidad a distancia con la finalidad de evitar contagios y mantener las medidas sanitarias aplicables para evitar su proliferación.

Importancia de la ciberseguridad en las Micro, Pequeñas y Medianas empresas (MiPymes)

COORDINACIÓN GENERAL DE POLÍTICA DEL USUARIO



Insurgentes Sur #1143 Col. Nochebuena
Demarcación Territorial Benito Juárez
C.P. 03720 Ciudad de México

Tel: 55 50154000 / 800 2000 120

www.ift.org.mx