Datasec

Estado de la Ciberseguridad en las empresas uruguayas

ENCUESTA 2023 - 2024

GRUPO RADAR
INTELIGENCIA DE MERCADO

Introducción

La ciber inseguridad se ha consolidado como uno de los principales riesgos para países y organizaciones, comparable con amenazas como el cambio climático, las crisis sociales y los conflictos bélicos. (Informe de Riesgo Global del WEF 2024).

Tanto a nivel global, como regional y en Uruguay, es evidente el incremento de incidentes graves de ciberseguridad que han captado la atención pública durante 2023. Este aumento no es sorpresivo.

En Datasec, con más de tres décadas dedicadas a la difusión del conocimiento en seguridad de la información y ciberseguridad, iniciamos hace más de siete años una colaboración con Grupo Radar. Nuestro propósito ha sido recabar datos objetivos que reflejen fielmente la situación de ciberseguridad en Uruguay, basándonos en el estudio del Perfil del Internauta Uruguayo.

Datasec

Nos focalizamos inicialmente en la ciberseguridad de los ciudadanos durante los primeros dos años y, posteriormente, hemos dirigido nuestra atención a las empresas en los últimos cuatro años. Este informe contribuye a esa serie, presentando datos concretos obtenidos de las empresas acerca de su madurez en ciberseguridad, la naturaleza de los incidentes experimentados, y la implementación de controles básicos.

A lo largo de los años, hemos observado una variabilidad en los datos, atribuible en gran parte a la ausencia de un referente específico de ciberseguridad en la mayoría de las empresas uruguayas y a la complejidad de ciertas preguntas, como el reconocer incidentes graves en el último año.

Sobre la base de los resultados, no debería sorprendernos que la situación empeore durante los próximos años. Entre las empresas que cuentan con

sitio web, realizan ventas por Internet y/o consideran el correo electrónico como una herramienta clave:

- El setenta y siete por ciento (77%) admite no tener políticas de ciberseguridad documentadas.
- El cuarenta y siete por ciento (47%) indica que no ofrece formación ni concienciación en ciberseguridad.
- El treinta y dos por ciento (32%) no aplica filtrado de correo electrónico.
- El catorce por ciento (14%) carece de antivirus.
- El cuarenta y uno por ciento (41%) no realiza copias de seguridad fuera de la empresa.

La ciberseguridad depende crucialmente de la calidad de la infraestructura tecnológica de las empresas, la capacitación de su personal y la madurez de sus procesos internos.

Ante una ausencia de liderazgos internos, infraestructuras y controles tecnológicos obsoletos, los problemas son una consecuencia lógica.
En este contexto es imperativo generar incentivos para la mejora y proporcionar soporte y financiamiento que permitan a las organizaciones abordar sus vulnerabilidades más críticas. La ciberseguridad es un desafío técnico, legal, educativo y, en gran medida, económico. Cabe destacar que un ochenta por ciento (80%) de las medianas y grandes empresas uruguayas considera que la ciberseguridad no es percibida como importante por sus clientes.

Cordialmente,

Ing. Reynaldo C. de la Fuente
Socio Director Datasec.
www.datasec-soft.com
reynaldo@datasec-soft.com

Ficha técnica

	UNIVERSO	MUESTRA
TOTAL	183.897	600
Grandes y medianas	8.613	207
Pequeñas y micro	175.283	393
Industria	25.891	116
Comercio	61.727	238
Servicios	96.278	246
Área metropolitana	102.245	297
Interior	81.651	303

Se aplicó una encuesta telefónica a una muestra aleatoria de 600 empresas, representativa del universo de todas las empresas uruguayas.

Se definieron cuotas según tres criterios:

Zona geográfica: Montevideo e Interior.
Tamaño de empresa: micro/pequeñas y medianas/grandes.
Sector de actividad: Industria, Comercio y Servicios.

Se sobre-muestrearon los segmentos con universos más reducidos: industria, y empresas medianas y grandes. A efectos del procesamiento de los resultados generales se le dio a cada segmento su peso real en el universo de empresas.

El margen de error máximo para la muestra general es de ±4.0, para un nivel de confianza del 95%.

El relevamiento de campo se realizó en el transcurso de noviembre y diciembre del año 2023.

Encuesta

Referencia de bases

BASE 1

Empresas con presencia en Internet (web, redes sociales, venden o reciben consultas en plataformas) o su correo electrónico es una herramienta importante en su trabajo.

BASE 2

Si la empresa tiene un responsable de la Ciberseguridad.

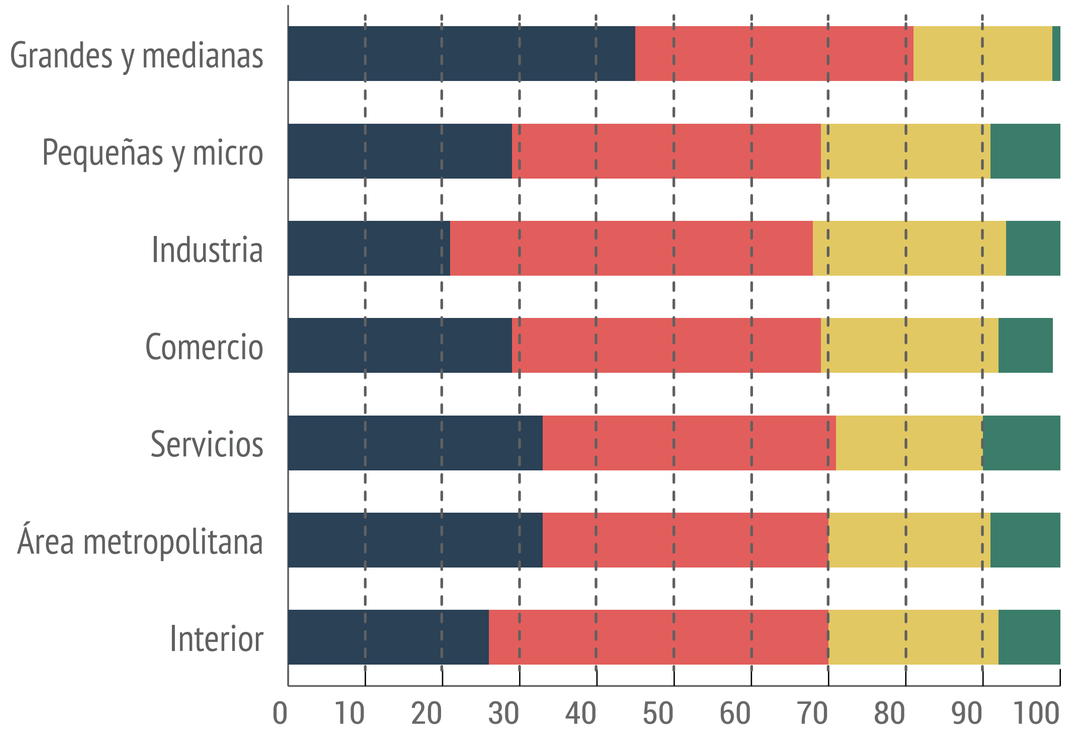
BASE 3

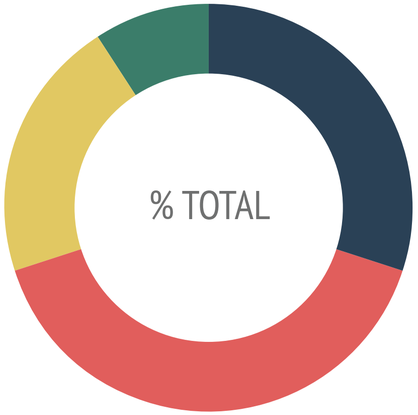
Empresas medianas y grandes que cuenten con página web, vendan por Internet y/o o su correo electrónico es una herramienta importante en su trabajo.

¿Cuánto le preocupa a su empresa los incidentes en seguridad de información?

Ejemplo: virus, hackeos, correos fraudulentos, robos o secuestros de información.

BASE 1

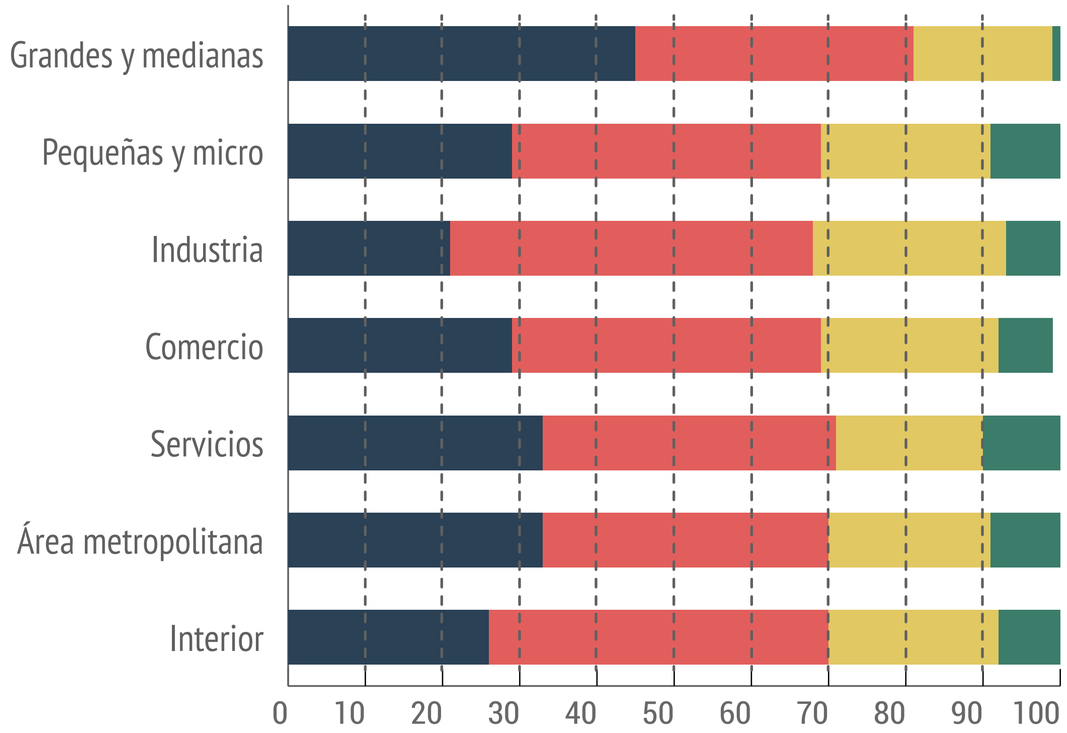


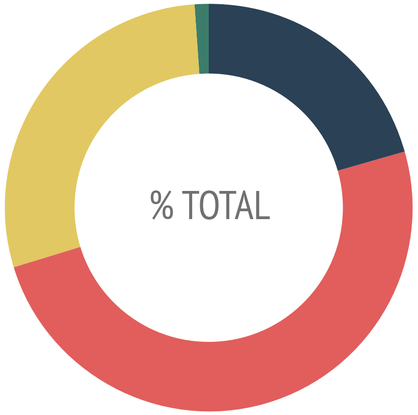


	2022
30% Me preocupa muchísimo	35%
40% Me preocupa bastante	43%
21% Me preocupa un poco	15%
9% No me preocupa nada	7%

¿Considera que su empresa ha tomado suficientes medidas para no ser víctima de incidentes de Ciberseguridad?

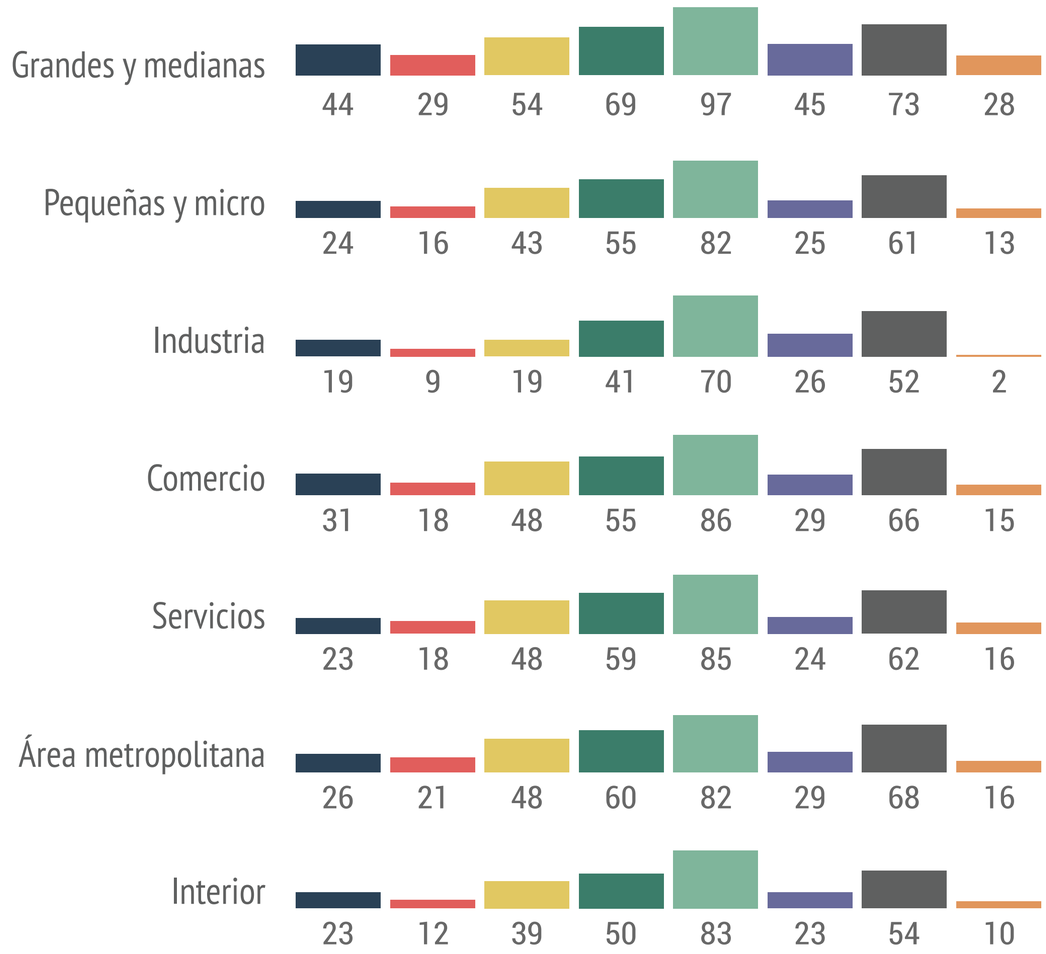
BASE 1





	% TOTAL	2022	2021
Sí, completamente	21%	34%	29%
Sí, parcialmente	50%	41%	35%
No	29%	23%	29%
No sabe	1%	2%	7%

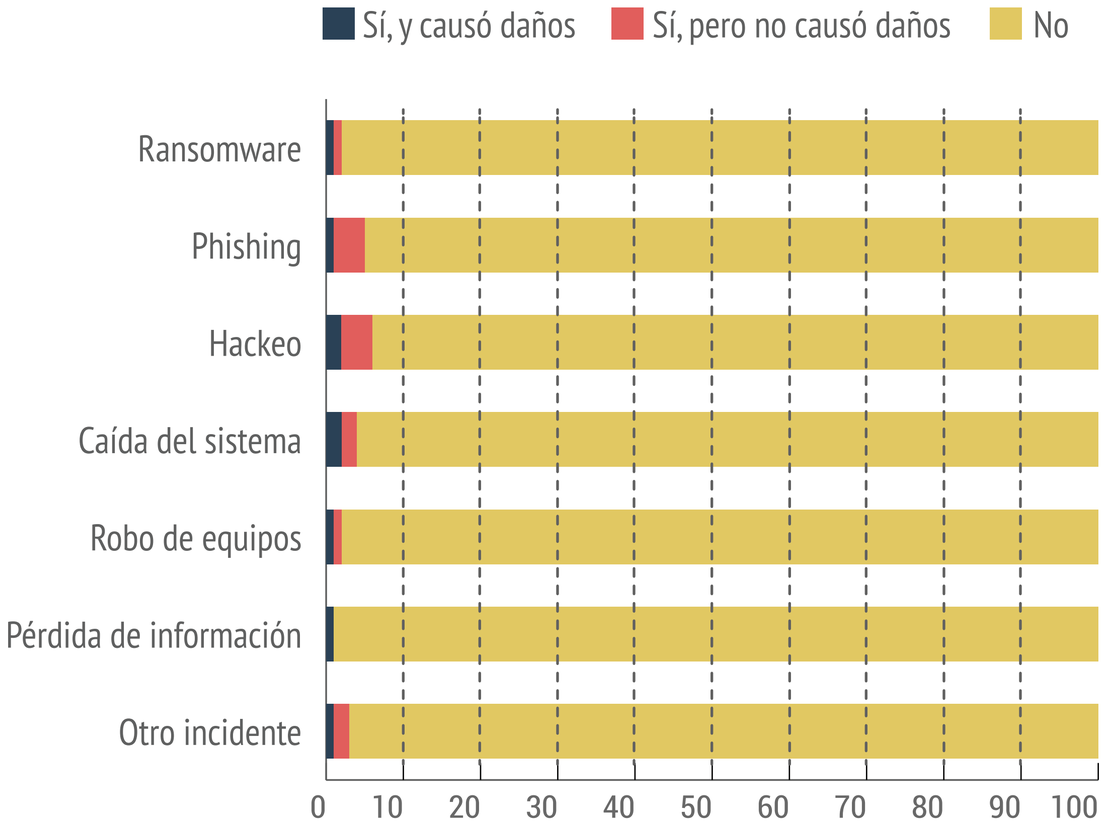
¿Qué controles de Ciberseguridad ha implementado? BASE 1



		2022	2021
Designaron un responsable de Ciberseguridad	25%	28%	30%
Cuentan con políticas de Ciberseguridad	17%	19%	20%
Concientizan a sus colaboradores	44%	47%	45%
Respaldan información en un sitio externo	55%	53%	59%
Cuentan con Antivirus	83%	81%	85%
Encriptan sus equipos portables	26%	30%	30%
Filtración de correos basura y fraudulentos	62%	59%	61%
2° Factor de autenticación para el trabajo remoto	14%	32%	21%

¿Su empresa ha sufrido alguno de estos incidentes en el último año?

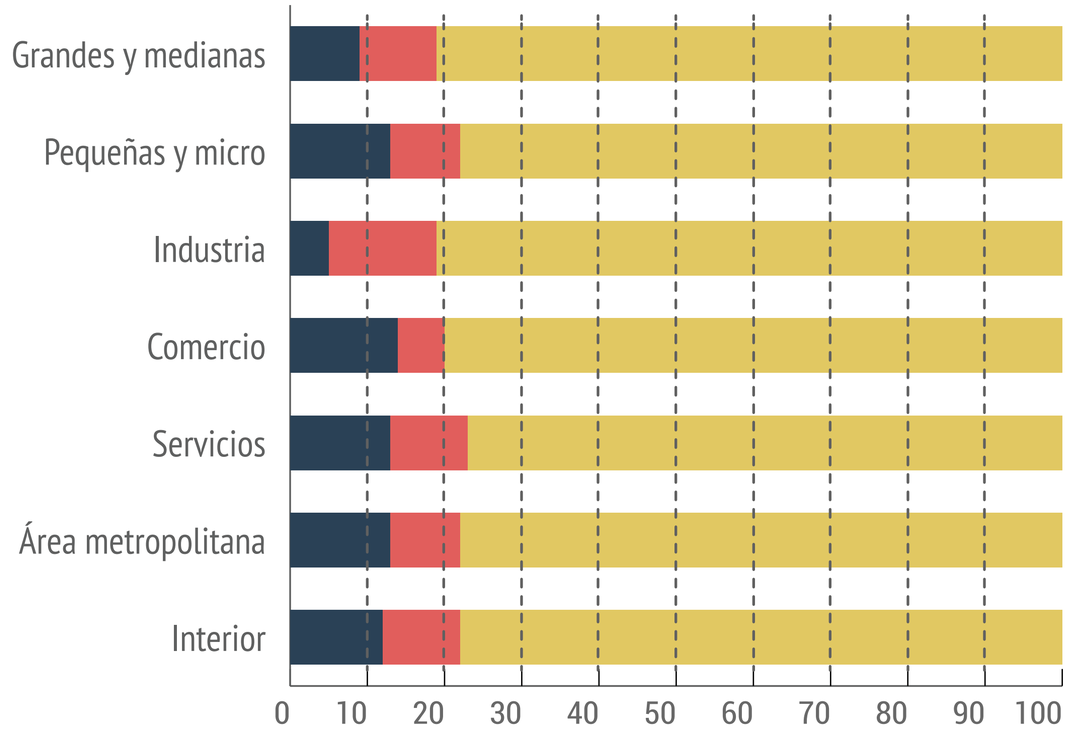
BASE 1

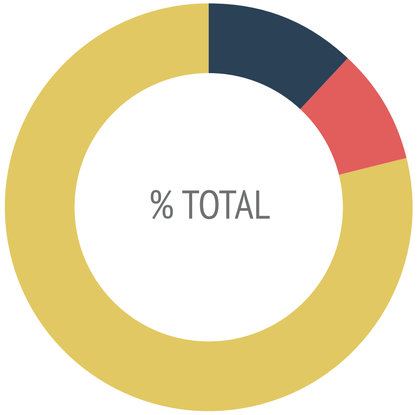


			2022	2021
Ransomware	2%	3.678 EMPRESAS	1%	2%
Phishing	5%	9.194 EMPRESAS	7%	0%
Hackeo	6%	11.033 EMPRESAS	4%	2%
Caída del sistema	4%	7.356 EMPRESAS	3%	6%
Robo de equipos	2%	3.678 EMPRESAS	2%	4%
Pérdida de información	1%	1.839 EMPRESAS	2%	3%
Otro incidente	3%	5.517 EMPRESAS	3%	

¿Conoce alguna empresa que haya tenido algún incidente grave de Ciberseguridad el último año pero que no haya sido publicado en la prensa?

BASE 1

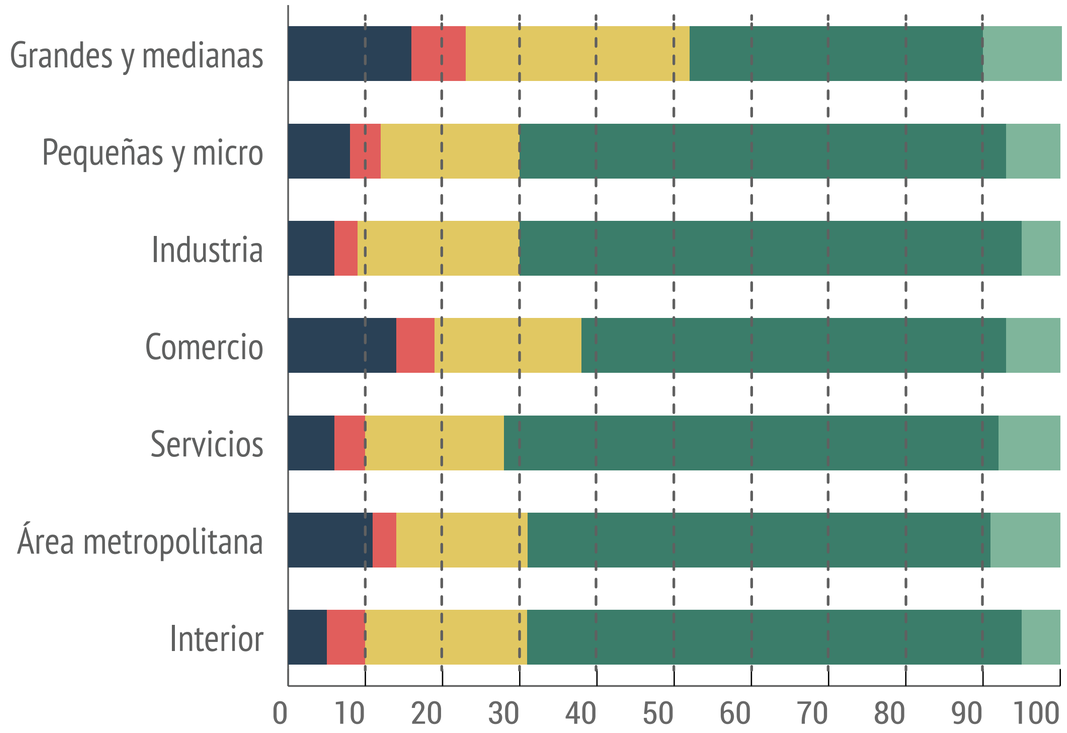


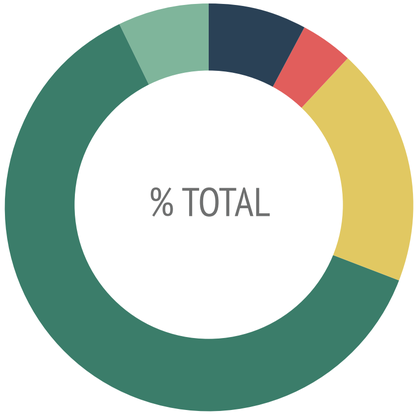


	2022
12% Sí, más de una	7%
9% Sí, una	10%
78% Ninguna	83%

¿Se ha realizado algún tipo de evaluación del estado de su Ciberseguridad?

BASE 1



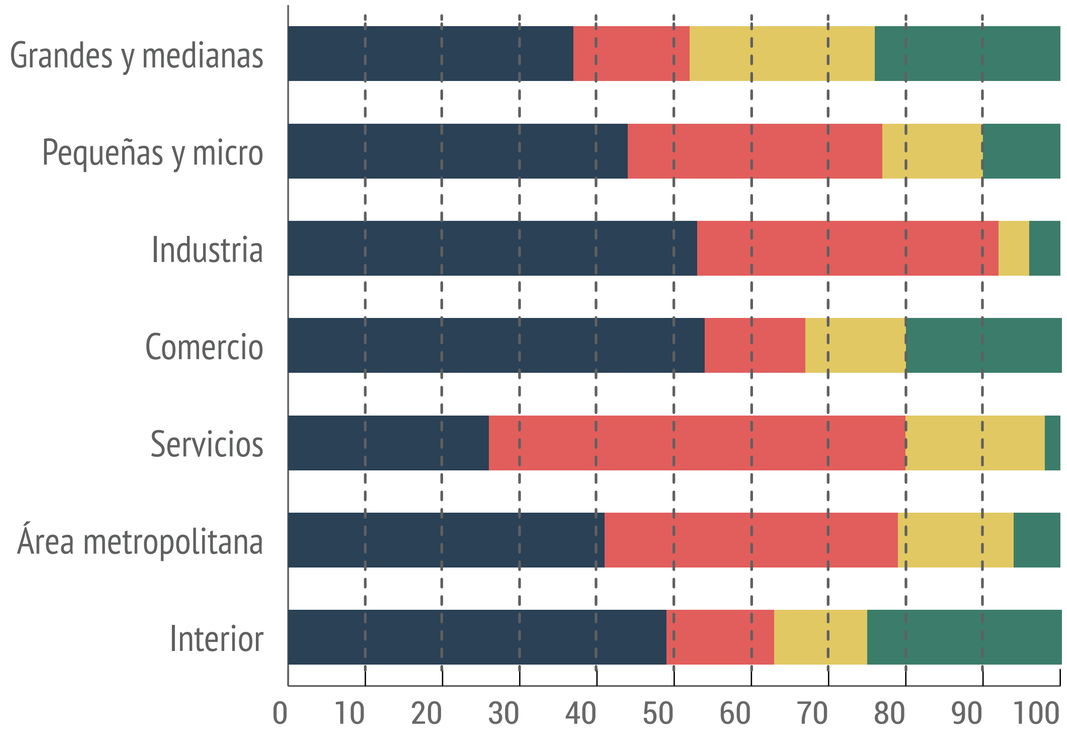


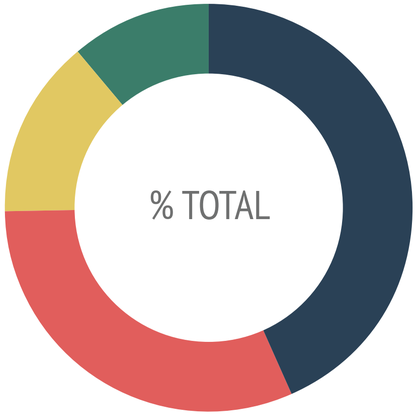
	2022	2021
8% Sí, regularmente	10%	12%
4% Sí, de forma excepcional	6%	6%
19% No, pero nos interesa hacerlo	14%	18%
62% No, y no lo consideramos necesario	63%	63%
7% No sabe	7%	

¿La empresa ha sido sometida a un hacking ético o escaneo de vulnerabilidad para evaluar su seguridad?

En sitios web, mails y aplicaciones expuestas a Internet, que contestaron “Sí, regularmente” en la respuesta anterior.

BASE 1

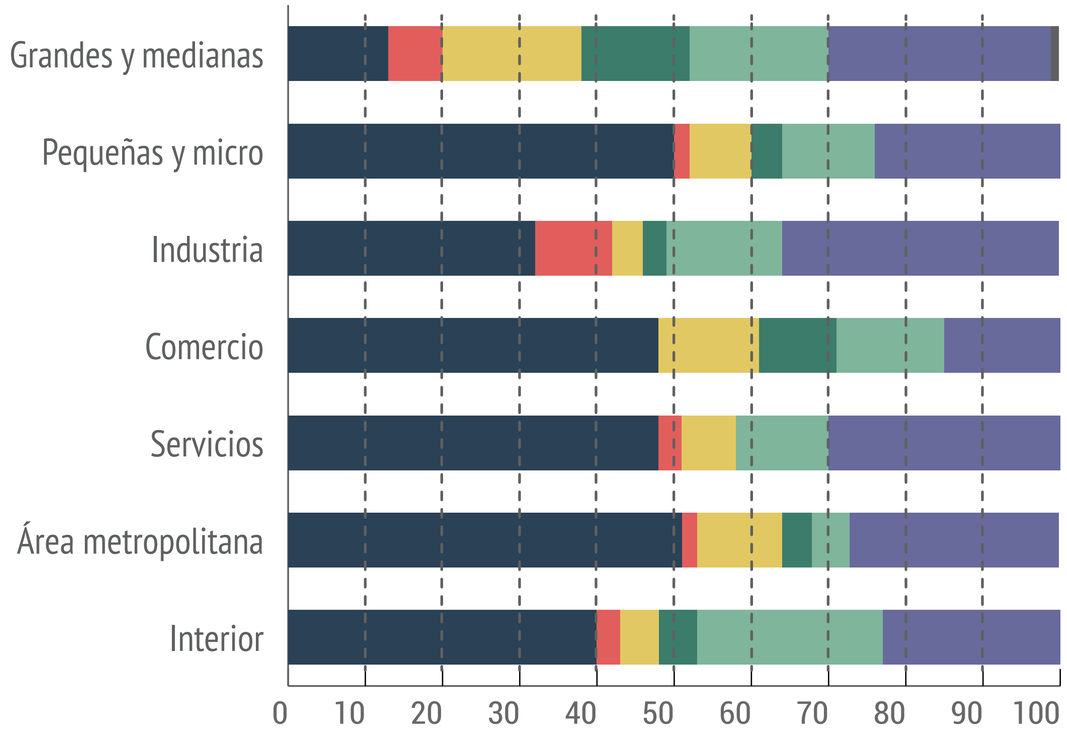


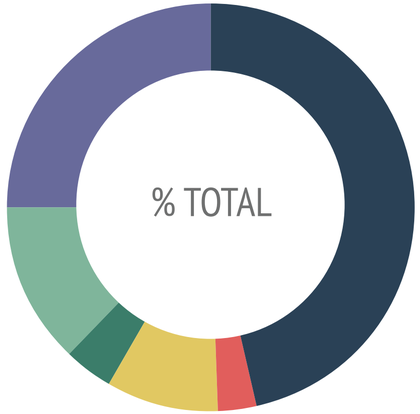


	2022	2021
43% Sí, de forma regular	38%	35%
31% Sí, de forma excepcional	11%	9%
14% No, pero nos interesa hacerlo	14%	13%
11% No, y no lo consideramos necesario	35%	43%

¿Quién es el/la responsable de la Ciberseguridad?

BASE 2

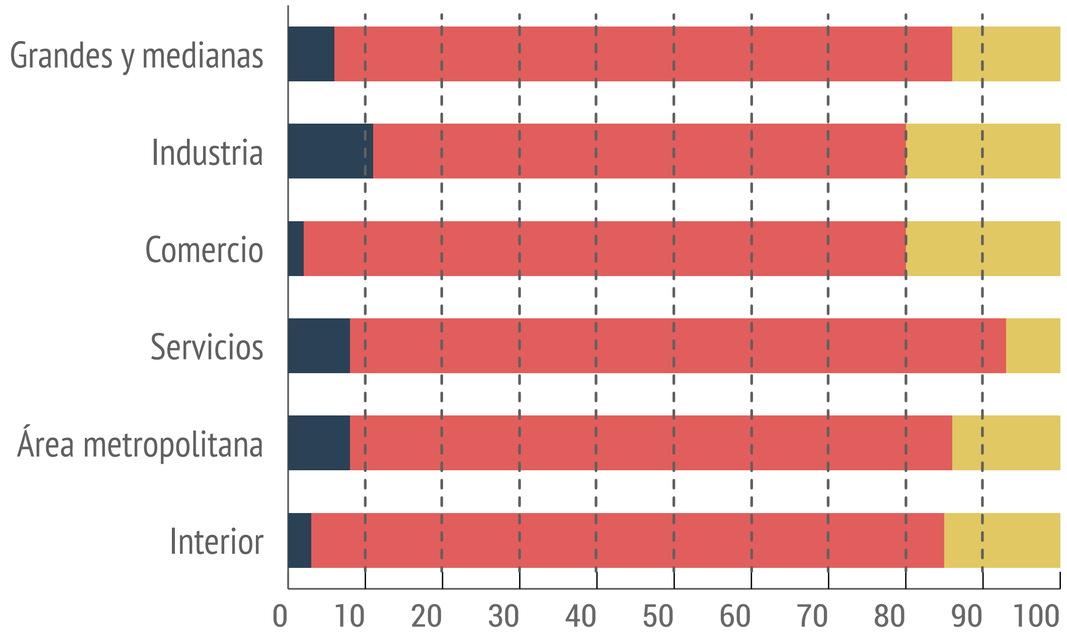


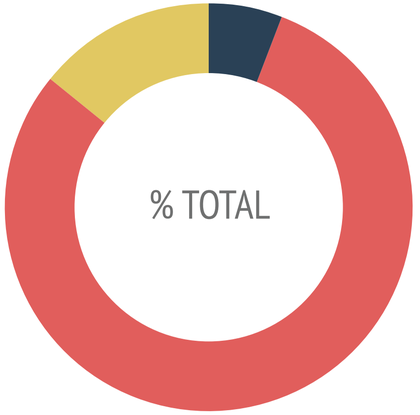


	2022	2021
47% Dueño o socio	32%	44%
3% Gerente general	6%	3%
9% Gerente de IT	4%	7%
4% Jefe de seguridad de la información	9%	8%
13% Otro cargo	19%	12%
25% Empresa o persona externa	28%	25%
0% No sabe	2%	3%

¿La empresa ha contratado un seguro para cubrirse ante incidentes de Ciberseguridad

BASE 3

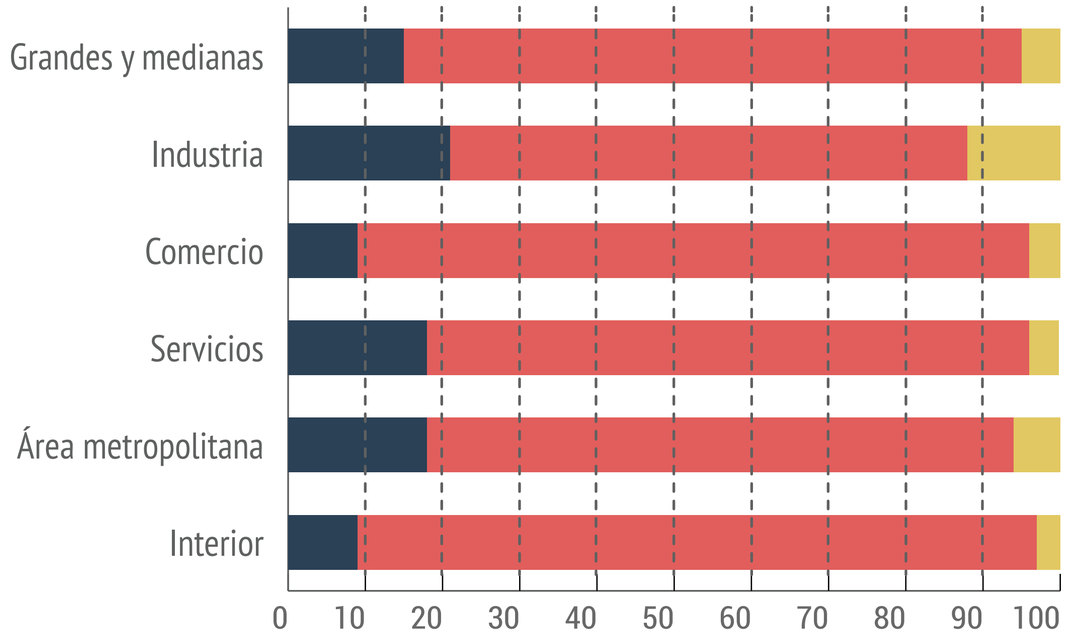


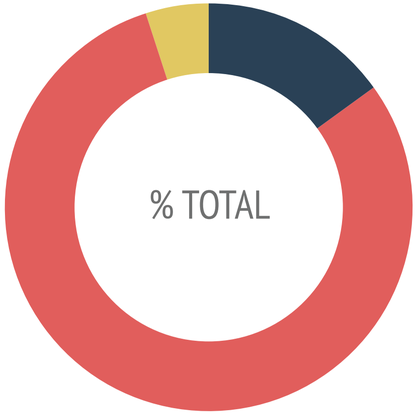


	2022	2021
6% Sí	14%	12%
80% No	79%	87%
14% No sabe	7%	1%

¿Los clientes de la empresa exigen niveles de Ciberseguridad importantes?

BASE 3

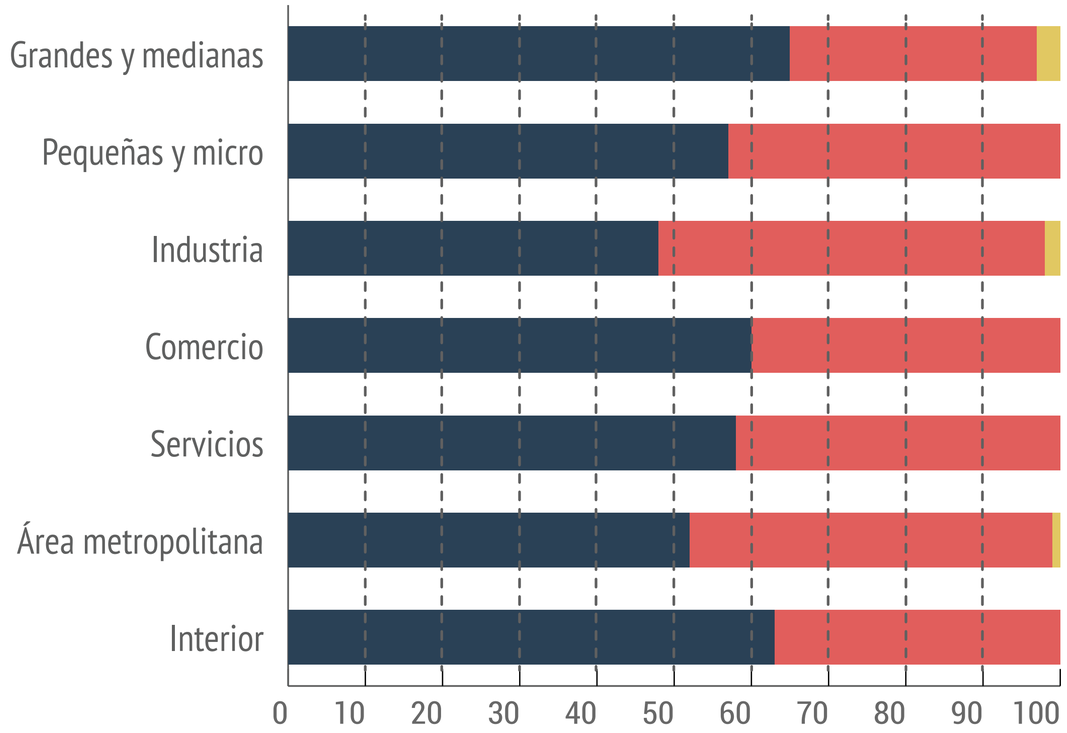


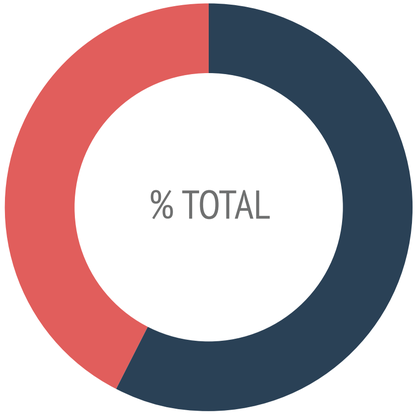


	2022
15% Sí	13%
80% No	84%
5% No sabe	4%

¿La empresa guarda datos personales de sus clientes?

BASE 1





	2022
57% Sí	52%
42% No	48%
0% No sabe	0%

Conclusiones

El análisis de los datos de 2023 sobre la ciberseguridad en empresas uruguayas desvela conclusiones importantes.

El número de empresas que sienten ansiedad sobre su nivel de preparación ha crecido, con solo un veintiún por ciento (21%) de las empresas afirmando que se siente completamente preparadas en materia de ciberseguridad. Hay una baja respecto del treinta y cuatro por ciento (34%) del 2022, lo cual es una buena noticia, ya que indica que las empresas están tomando mayor conciencia de su verdadero estado de situación, y los incidentes que han tomado carácter público han permitido visualizar de mejor forma la dimensión que un incidente grave puede tener para las organizaciones.

Lo que resta aún es que esta toma de conciencia se traduzca en acciones concretas. De las empresas que cuentan con sitio web, realizan ventas por Internet y/o consideran el correo electrónico como una herramienta clave, el cincuenta y siete por ciento (57%) reconocen mantener datos personales de sus clientes, pero un ochenta y un por ciento (81%) no realiza ningún tipo de evaluación de la situación de su ciberseguridad ya sea de forma esporádica o regularmente.

A modo de dato final, hoy hay en Uruguay doscientos cincuenta (250) empresas medianas que no cuentan con ningún tipo de antivirus, no filtran los correos electrónicos, no brindan charlas de concientización de ningún tipo o cuentan con políticas de seguridad de la información o ciberseguridad. Si tomáramos un criterio externo, ya fueron hackeadas, pero no lo saben.

A través de este informe, Datasec aspira a aportar claridad e información relevante, subrayando la necesidad crítica de abordar los riesgos de ciberseguridad con seriedad y previsión. En un panorama cada vez más desafiante, es vital que las organizaciones se detengan a considerar cómo gestionan y protegen tanto los datos sensibles de sus clientes como su propia información interna.

La confianza digital emerge como un pilar fundamental en nuestro mundo, donde las operaciones y las comunicaciones dependen cada vez más de los medios digitales. Esta confianza, arraigada en la seguridad y en la percepción de seguridad por parte de usuarios, consumidores y organizaciones, se forja sobre principios clave como la seguridad de la información, la privacidad, la transparencia y la responsabilidad en el tratamiento de datos y procesos digitales.

Para las empresas uruguayas, la adopción de enfoques proactivos y la inversión en niveles de ciberseguridad adecuados son pasos fundamentales hacia la consolidación de esta confianza digital.

Ing. Reynaldo C. de la Fuente

Socio Director Datasec.

www.datasec-soft.com

reynaldo@datasec-soft.com

Datasec

www.datasec-soft.com