Datasec

GRUPO RADAR
INTELIGENCIA DE MERCADO

ENCUESTA

Estado de la Ciberseguridad en las empresas uruguayas

2020 - 2021

INTRODUCCIÓN

El año 2020 sin duda será recordado como un año de importantes desafíos para la continuidad operativa de las organizaciones. En este contexto, lamentablemente la ciberseguridad no ha sido una excepción, sino un agravante que se sumó a un escenario ya complejo.

El vertiginoso ascenso del nivel de riesgo de ciberseguridad es una clara consecuencia de la rápida digitalización y el crecimiento del teletrabajo durante la pandemia, que aumentó la exposición creando redes más complejas y potencialmente menos seguras. De acuerdo con el informe 'Force Threat Intelligence Index 2021', a nivel mundial, el ransomware fue el tipo de amenaza más importante, significando el 23% de los ataques. El escaneo de vulnerabilidades y explotación de estas fue el vector de ataque número uno, superando el phishing, el principal vector en 2019.

Es claro que el desconcierto y el teletrabajo han dejado un terreno muy fértil para que los ciberdelincuentes desarrollen sus habilidades y se aprovechen la situación para incrementar sus ataques de suplantación de identidad, ransomware de doble extorsión y explotación de vulnerabilidades. Estos escenarios se han multiplicado significativamente, dejando a organizaciones de todos los sectores muy vulnerables y en muchos casos con graves problemas operativos y financieros.

En este contexto y en el marco de nuestro compromiso con la concientización en seguridad de la información hemos realizado una nueva encuesta para relevar cómo se han preparado las organizaciones en Uruguay para enfrentar esta creciente amenaza, y conocer si han sido afectadas por algún incidente de seguridad en el último año.

La gran mayoría de las organizaciones no tiene los controles necesarios y terminan siendo víctimas de los ciberataques, algo que en muchos casos ni siquiera son capaces de identificar para protegerse a tiempo.

La seguridad de la información y ciberseguridad significa un riesgo operativo en crecimiento en todo el mundo, tanto así que el informe del foro económico mundial publicado en 2021 lo ubica en el 4to lugar del ranking, muy por encima del terrorismo y el cambio climático.

LA CIBERSEGURIDAD

Distintos informes realizados a nivel mundial destacan a los riesgos de Ciberseguridad como uno de los principales riesgos operativos que enfrentan las empresas a nivel global este escenario no elude a la realidad uruguaya en la cual cada año son más las empresas que sufren eventos e incidentes con impacto importante para su operativa y sus clientes.

Recientemente la legislación uruguaya fue actualizada incorporando nuevas obligaciones para la protección de los datos personales de los uruguayos por parte de las empresas entre estas obligaciones se destacan el que la empresa lleva adelante acciones proactivas para evitar ser víctima de un incidente Asimismo las empresas deberán reportar los incidentes que afecten los datos personales de los uruguayos al centro de respuesta de incidentes de AGESIC.

En este contexto el presente informe busca aportar información sobre el escenario de las empresas y al mismo tiempo estimular a que estas implementen las más mínimas prácticas necesarias para garantizar su ciberseguridad así como la de sus clientes destacando la privacidad y protección de sus datos personales.

Las preguntas realizadas a lo largo de esta encuesta buscan determinar si las empresas fueron víctimas de los principales incidentes de Ciberseguridad que actualmente se conocen a nivel global y al mismo tiempo identificar el grado de madurez que estas presentan respecto de los más mínimos controles necesarios para hacer frente a los riesgos existentes.

Qué tan seguros estamos en materia de Ciberseguridad, es una pregunta que muchas empresas no son capaces de contestar adecuadamente la respuesta. En muchos casos es subjetiva basada en la percepción de sus directores o dueños, nunca nos pasó nada, si este año tuvimos varios incidentes no es un claro indicador de la realidad que la empresa está enfrentando la ausencia total o parcial de indicadores roles y responsabilidades específicas en la materia hace que muchas empresas tengan un claro desconocimiento de su realidad.

FICHA TÉCNICA

Se aplicó una encuesta telefónica a una muestra 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 excluyó el sector primario del estudio, por tratarse de un universo demasiado reducido.

Se sobremuestrearon los segmentos con universos más reducidos, como industria, y empresas medianas y grandes.

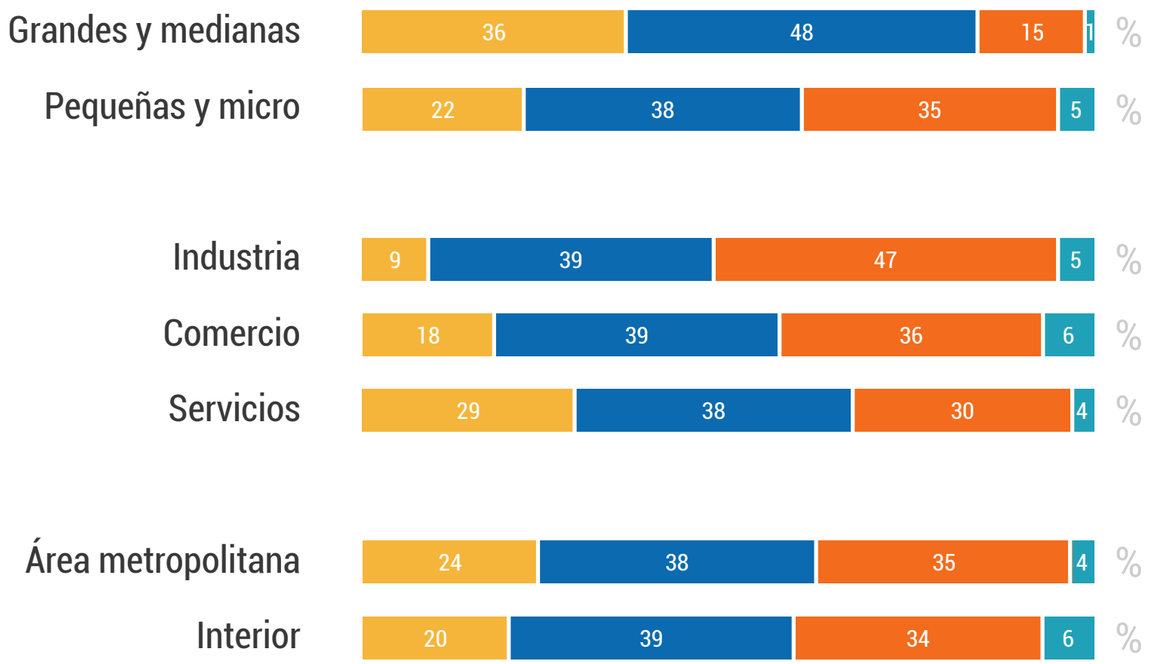
A efectos del procesamiento de los resultados generales se le dio a cada segmento su peso real en el universo de empresas.

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

	UNIVERSO	MUESTRA
TOTAL	**172133**	**619**
Grandes y medianas	6100	236
Pequeñas y micro	166034	383
Industria	25280	107
Comercio	60198	257
Servicios	86656	255
Área metropolitana	96963	312
Interior	75170	307

¿Considera que su empresa se encuentra preparada ante incidentes de Ciberseguridad?

Virus, hackeos, robos o secuestros de información.



2019

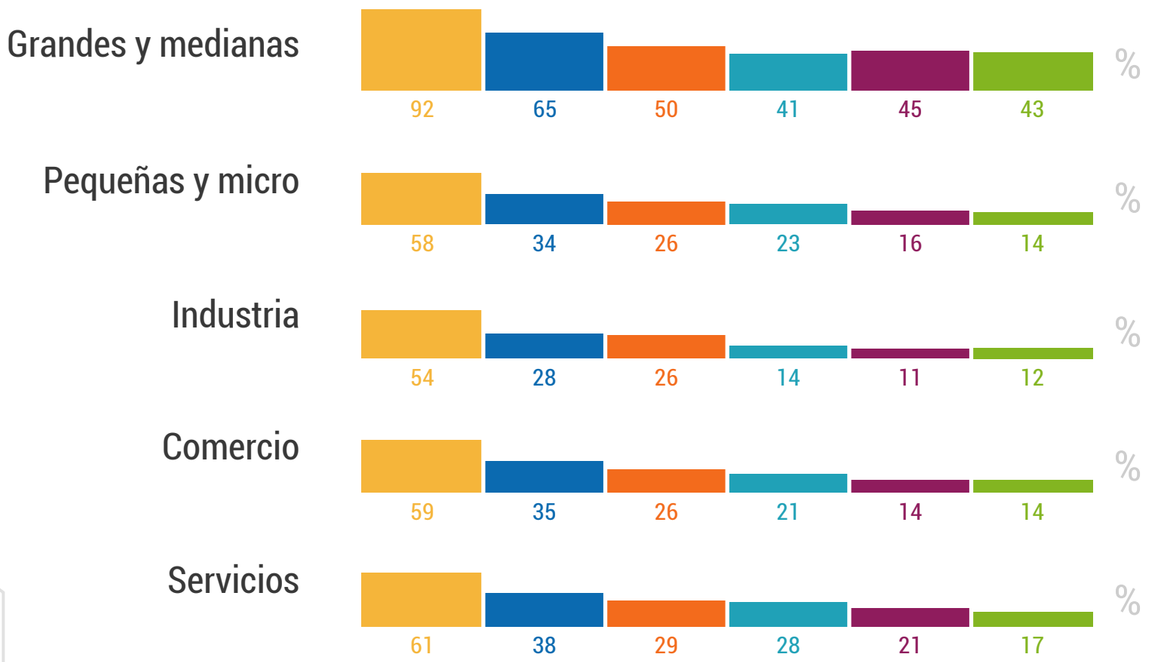
22%
Sí, completamente
22%

38%
Sí, parcialmente
27%

35%
No
39%

5%
No sabe
12%

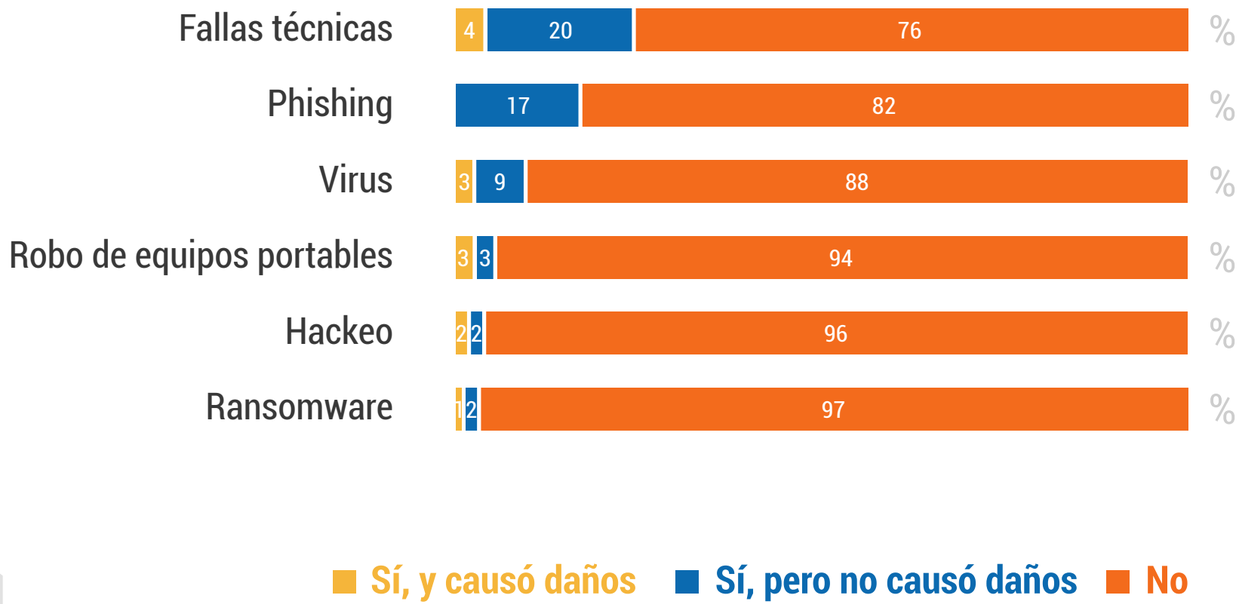
¿Qué controles de Ciberseguridad se han implementado?

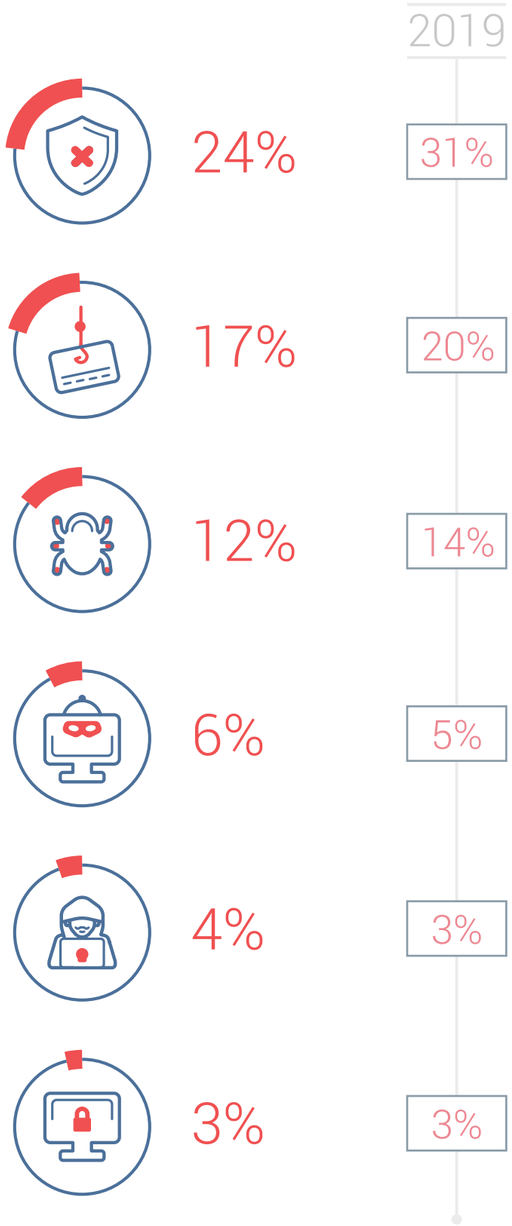


	2019
Cuentan con Antivirus	59%
Respaldan información en un sitio externo	35%
Concientizan a sus colaboradores	27%
Encriptan sus equipos portables	23%
Designaron un responsable de Ciberseguridad	17%
Cuentan con políticas de Ciberseguridad	15%

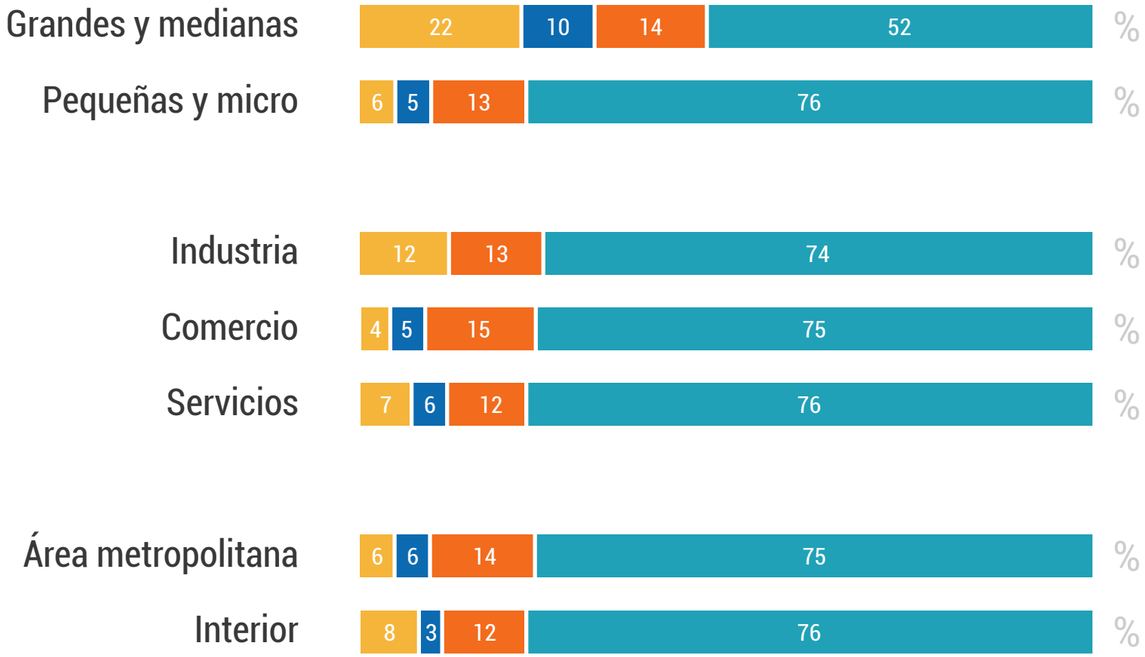
77%
57%
42%
20%
29%
22%

¿Qué incidentes de Ciberseguridad tuvieron el último año?





¿Se han sometido a algún tipo de evaluación del estado de su Ciberseguridad?



2019

7%
Sí, regularmente
5%

5%
Sí, de forma excepcional
3%

13%
No, pero les interesaría
14%

75%
No, y no lo creen necesario
77%

¿Han sido sometidas a un hacking ético o escaneo de vulnerabilidad para evaluar su Ciberseguridad?

11%
Sí, de forma regular

16%
Sí, de forma excepcional

49%
No, y no lo creen necesario

24%
No, pero les interesaría

2019

6%

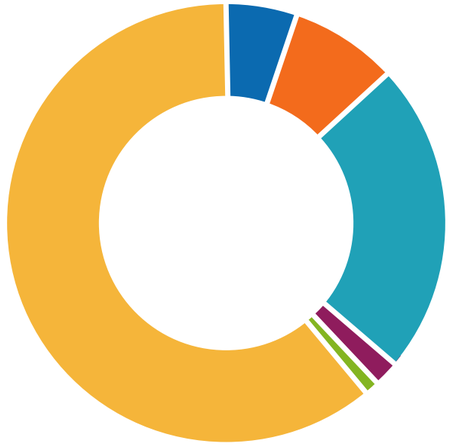
4%

18%

72%

Menos de 1/3 de empresas que se han sometido a evaluación de su seguridad, se sometieron a un hacking ético.

¿Quién es el/la responsable de la Ciberseguridad?



Grandes y medianas	24	6	26	33	9	1	%
Pequeñas y micro	64	4	6	23	3	1	%
Industria	62	1	4	31		1	%
Comercio	58	3	10	16	10	3	%
Servicios	61	5	7	26			%
Área metropolitana	62	2	9	25		2	%
Interior	58	8	5	21	6	2	%

60%
Dueño o socio

4%
Gerente general

7%
Gerente de IT

24%
Jefe de seguridad de la información

3%
Empresa contratada

1%
Otro cargo con conocimiento

2019

42%

7%

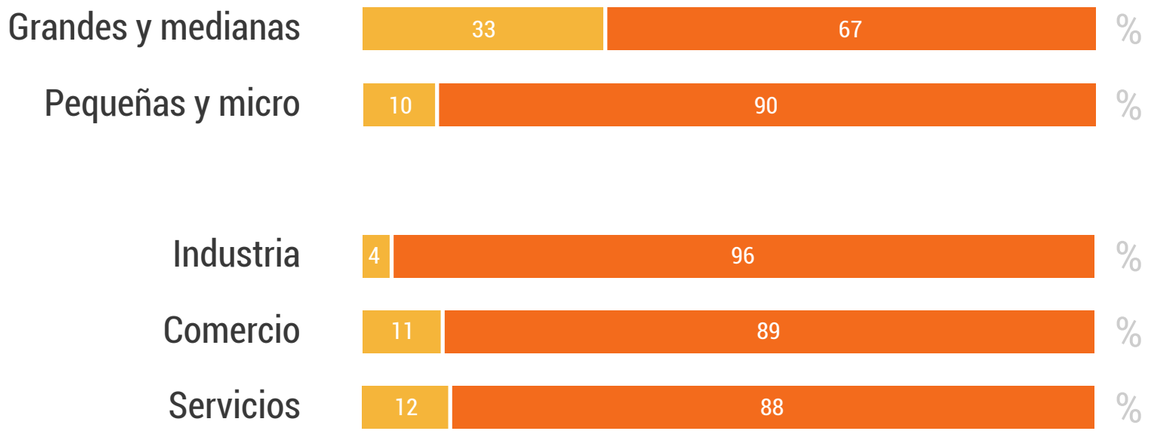
5%

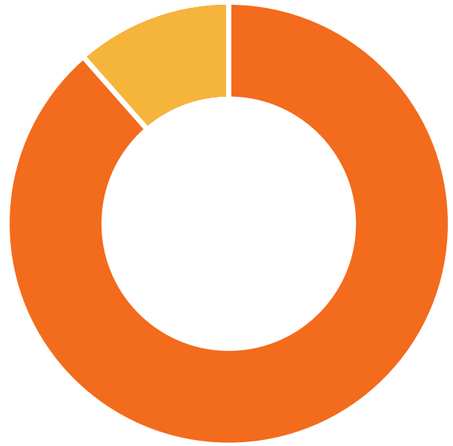
4%

27%

16%

¿Se ha designado a alguien para cumplir con la función de Delegado de Protección de Datos?



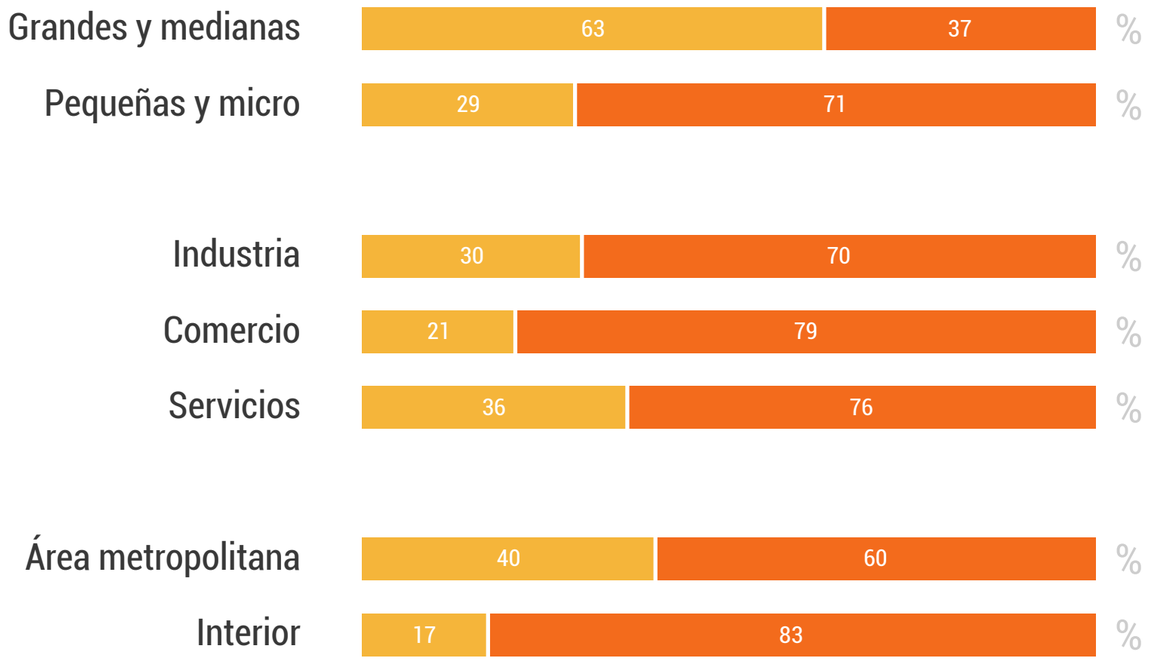


10%
Sí

90%
No

Debido a la emergencia sanitaria

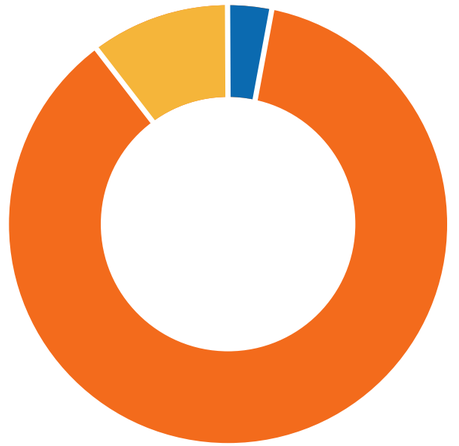
¿Hubo personal de la empresa que pasó a trabajar a distancia?

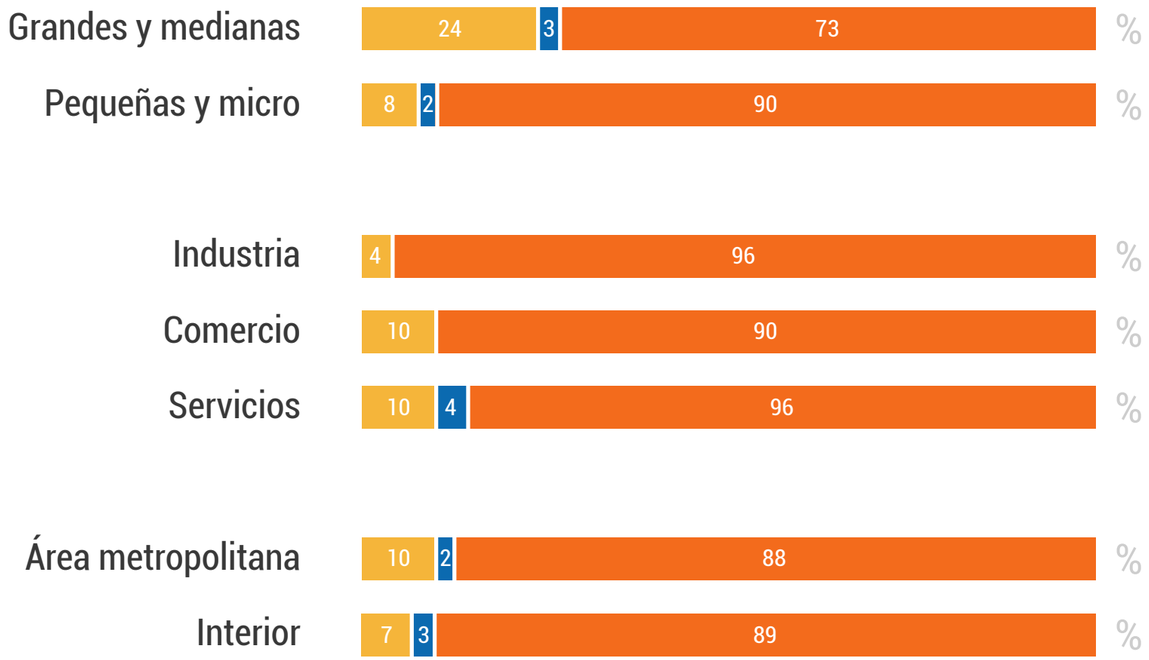


30%
Sí

70%
No

¿Cambiaron en algo las medidas de Ciberseguridad por tener personal trabajando a distancia?





9%
Se incrementaron

2%
Se flexibilizaron

89%
No cambiaron

CONCLUSIONES

Entendemos que, si bien se ha incrementado la conciencia en cuanto a las importantes amenazas existentes en materia de ciberseguridad, actualmente existe una falsa percepción de que la situación está controlada.

Lo cierto es que no hay ninguna evidencia de que el bajo nivel de incidentes reportados se deba a la implementación de controles y no a la gracia de la fortuna o un total desconocimiento del escenario que se enfrenta y en los hechos sufre.

Analizando los números observamos que, si bien un 60% de las organizaciones encuestadas indican que se encuentran preparadas ante un incidente de seguridad, cuando analizamos la implementación de controles básicos, un 75% del total no cuenta con ellos.

Por otra parte, si bien se ha profundizado en controles técnicos específicos como el antivirus o los respaldos, la gran mayoría de las organizaciones deja de lado la gobernanza de la seguridad de la información, siendo esta una cuestión crítica a la hora de mejorar la ciberseguridad.

Las políticas de seguridad y una evaluación de riesgos adecuada son el marco para una implementación eficiente de controles. En este mismo contexto, uno de los controles más importantes y menos costoso ha sido dejado de lado por la mayoría de las organizaciones (75%); que no realiza ningún tipo de acciones de concientización del personal. Las personas son el eslabón más débil de toda esta cadena y el principal vector que explotan los atacantes cuando una organización es vulnerada.

La seguridad de la información y ciberseguridad no es solamente una cuestión técnica, es un tema de gobernanza, compromiso y cumplimiento que alcanza a todo tipo de organización y a todos sus miembros, permeando en todas las esferas y alcanzando desde pequeñas acciones como la definición de una política o una charla, hasta autoevaluaciones técnicas como un escaneo o hacking ético.

Los incidentes ocurren y ya están golpeando la puerta de nuestros vecinos. Está en cada organización dejar de tentar la suerte y comenzar a tomar medidas eficaces.

Datasec es una empresa uruguaya con 30 años de historia, pionera para la región en gestión de riesgos y resiliencia organizacional.
El objetivo de este informe es generar información local, que ayude a conocer nuestra realidad y al mismo tiempo generar conciencia sobre el escenario que enfrentan las organizaciones en materia de Ciberseguridad.

Estamos a las órdenes ante cualquier consulta o solicitud de reunión a los efectos de evaluar sus objetivos, riesgos y requisitos en nuestra materia de especialidad.

Datasec

www.datasec-soft.com