Vulnerabilidad de Empresas en Ciberseguridad
Noviembre 2016

Bernardita Silva A.
Directora Ejecutiva OCI Chile
Cámara Nacional de Comercio

Sebastián Palacios
Director Jurídico de Asuntos P.I.
Microsoft

Objetivos

- Conocer el nivel de vulnerabilidad tecnológica de las empresas en relación a incidentes cibernéticos, indagando en las medidas que han sido implementadas para enfrentarlos.

De manera específica, el estudio abordará los siguientes temas:

- **Definir y cuantificar el perfil de la empresa en relación a:**
  - N° de trabajadores/empleados
  - N° de usuarios de PC/notebooks o similares.
  - Conexión a Internet
  - Conexión remota a servidores de la empresa
  - Área de TI/ encargados del área
  - Programas que son utilizados en la empresa
  - Restricciones para acceder a Internet

Objetivos

- ✓ **Experiencias de incidentes cibernéticos**
- ✓ **Antivirus y claves de acceso**
- ✓ **Uso de programas gratis**
- ✓ **Información sobre Cloud / Nube**

Metodología

Tipo de estudio → **Cuantitativo – Descriptivo**

Técnica → Encuesta, telefónica en base a un cuestionario estándar, diseñado principalmente con preguntas cerradas, con una duración de 10 minutos en su aplicación.

Target → Ejecutivos - responsables de las áreas de : administración / finanzas / informática de empresas medianas y pequeñas (PYMES), localizados en el Gran Santiago, Gran Valparaíso y Gran Concepción.

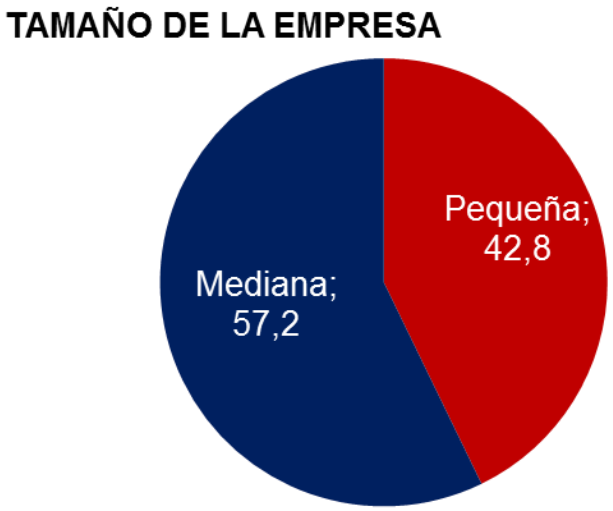
Muestra → Se realizaron 612 entrevistas distribuidas de la siguiente forma:

- Gran Santiago → 202
- Gran Valparaíso → 205
- Gran Concepción → 205

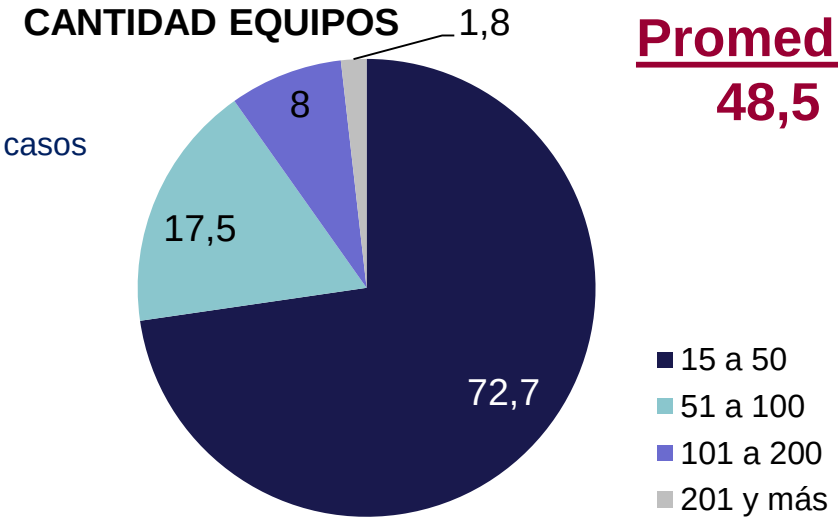
Trabajo de campo → Se realizó entre el 20 de Agosto y el 20 de Octubre, 2016

Principales Resultados

Contexto general

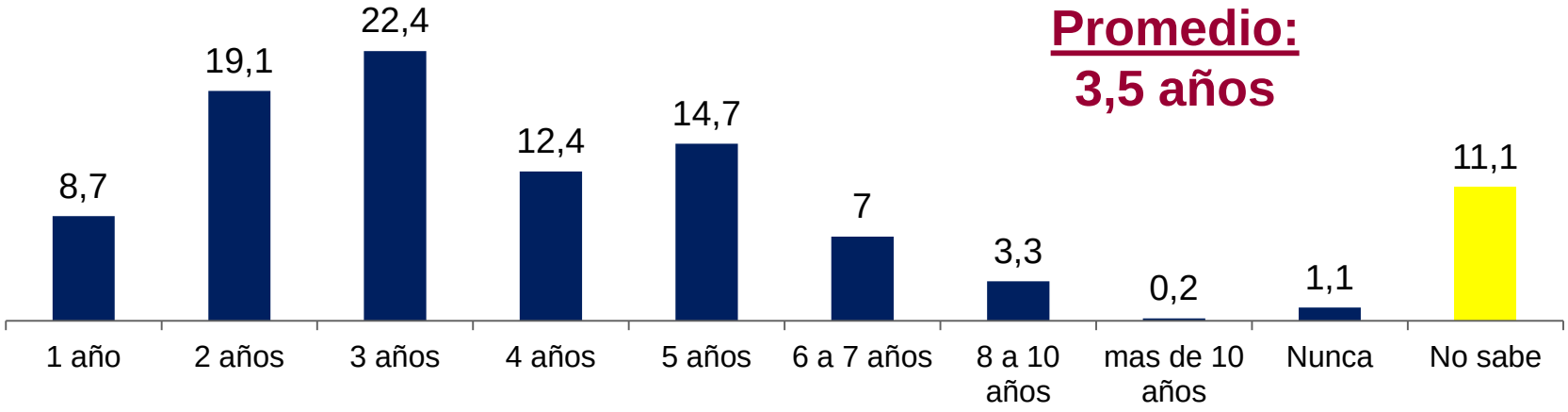


Base: 612 casos



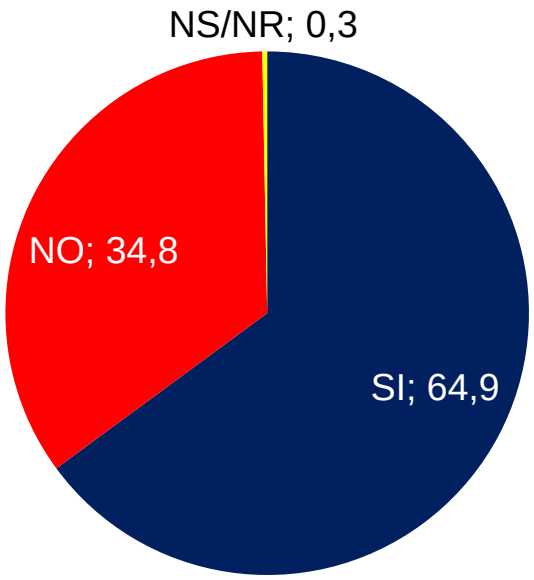
Promedio: 48,5

¿CADA CUÁNTO CAMBIAN LOS EQUIPOS?



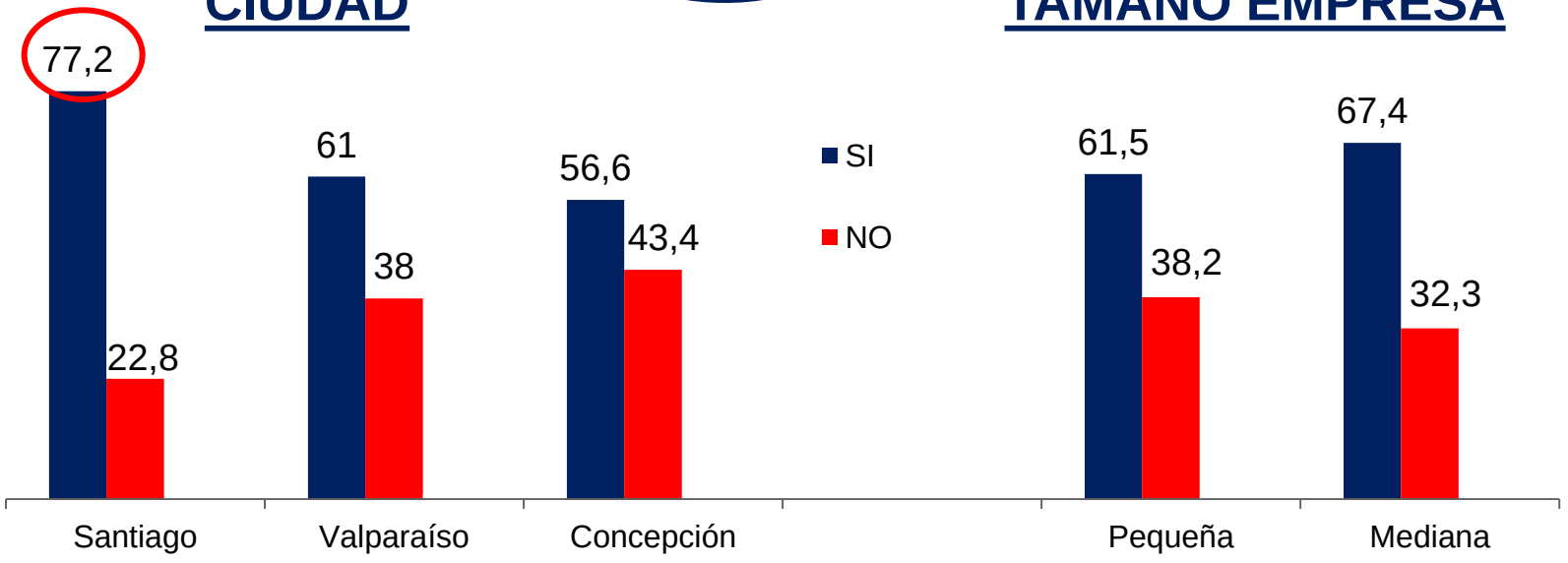
Promedio: 3,5 años

Conexión remota



Base: 612 casos

CIUDAD

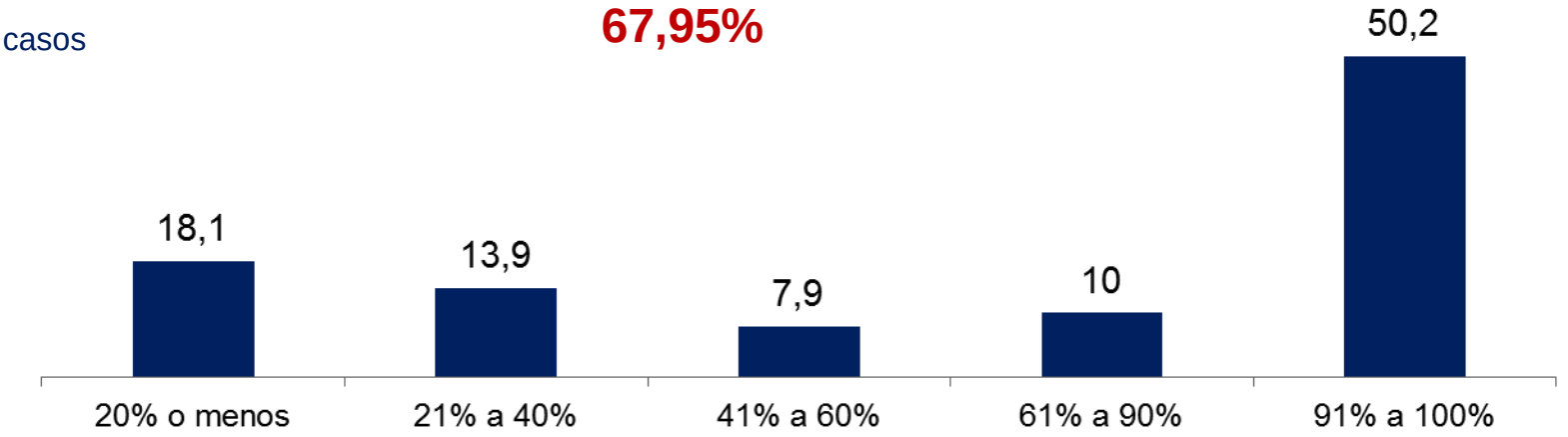


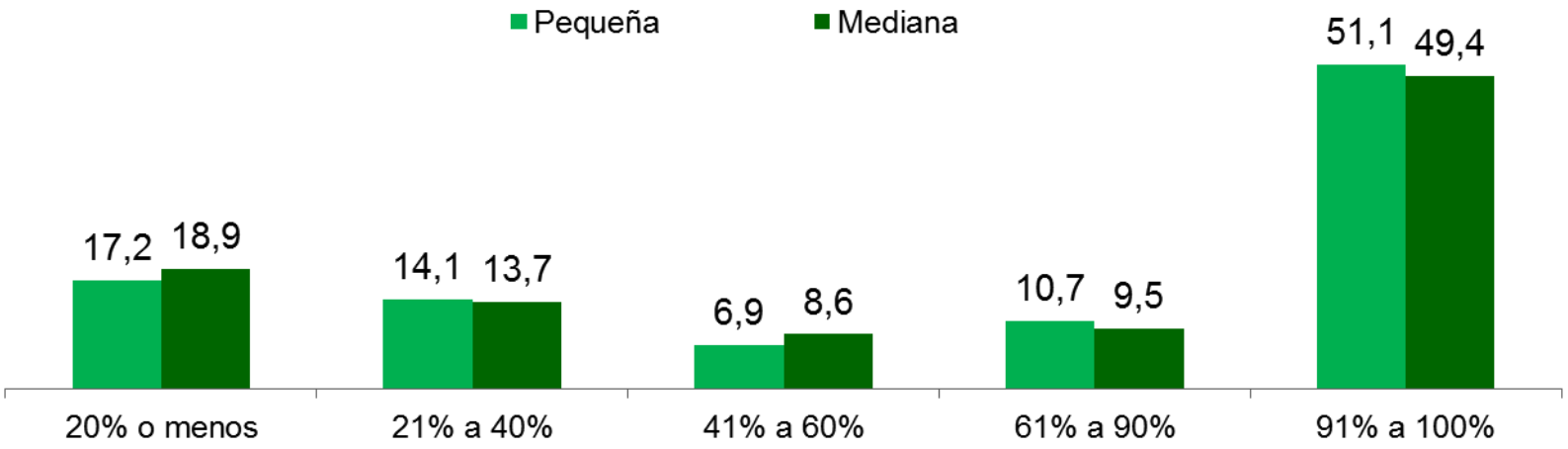
TAMAÑO EMPRESA

% Trabajadores con acceso a Internet

PROMEDIO
67,95%

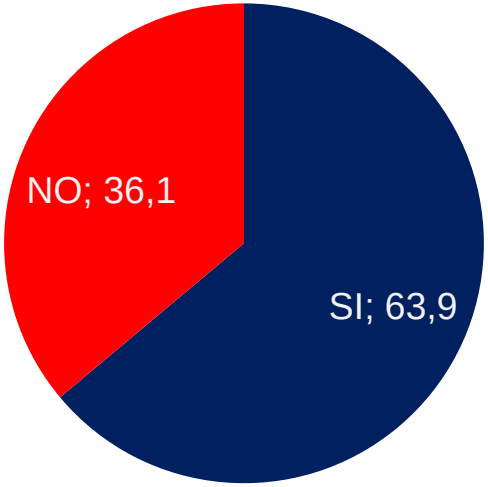
Base: 612 casos



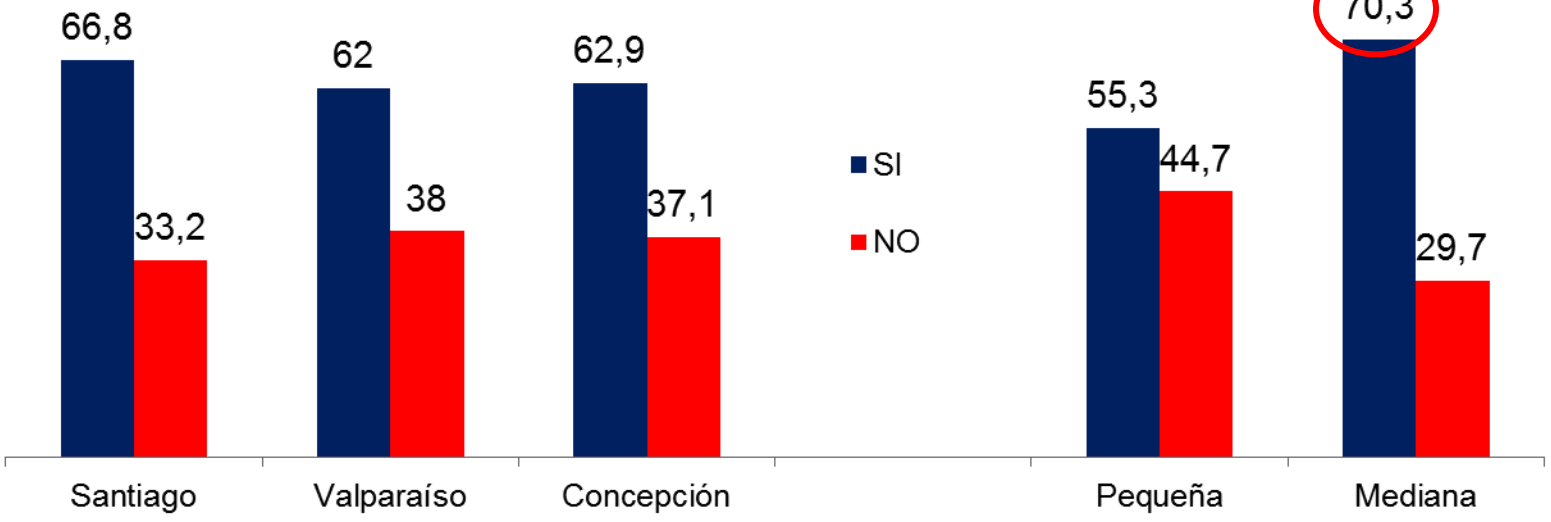


Restricciones para acceder a Internet

Base: 612 casos



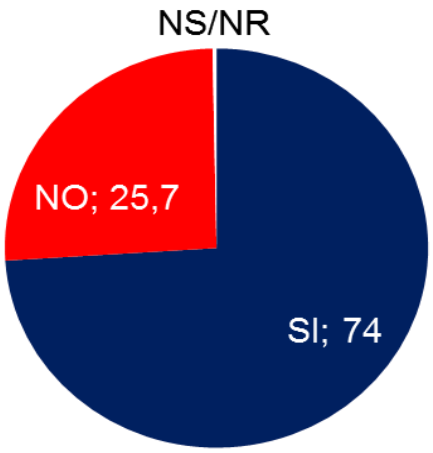
CIUDAD



TAMAÑO EMPRESA

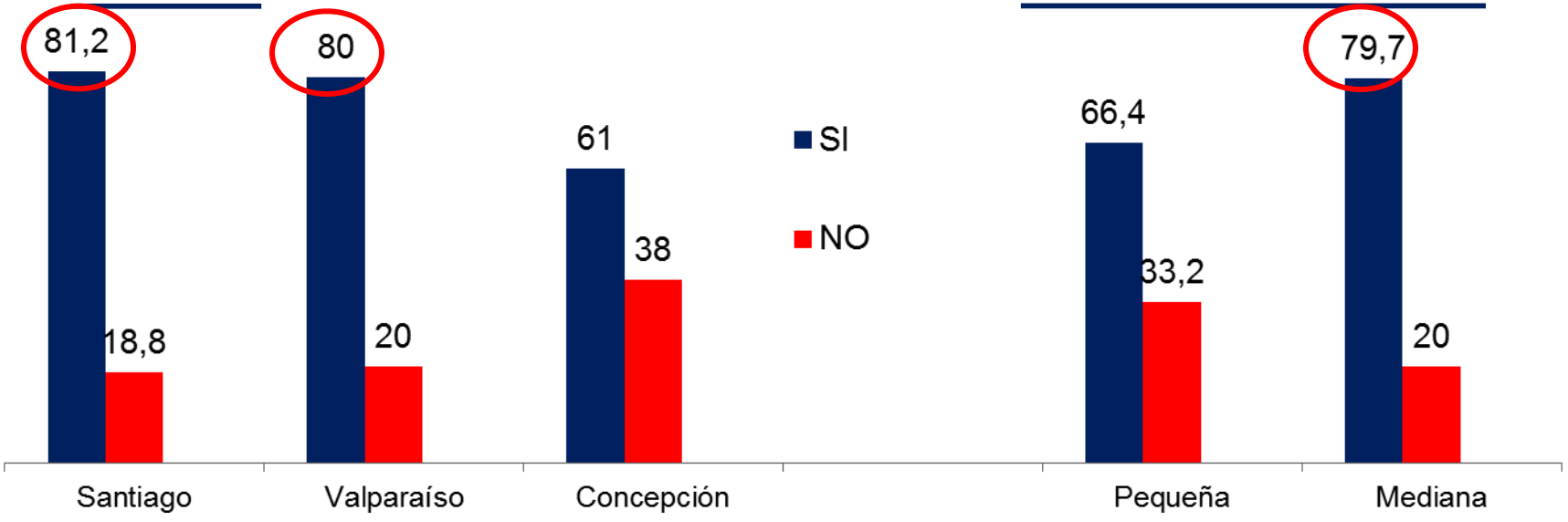
¿Tienen área o encargado de TI?

Base: 612 casos



CIUDAD

TAMAÑO EMPRESA

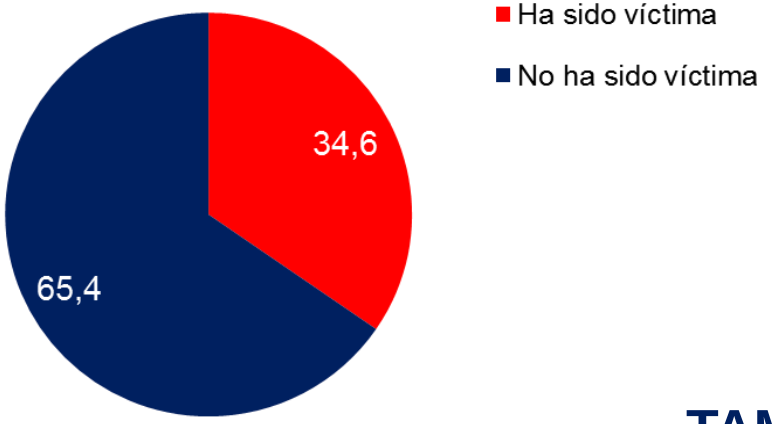


Experiencia con incidentes

Incidentes de ciberseguridad

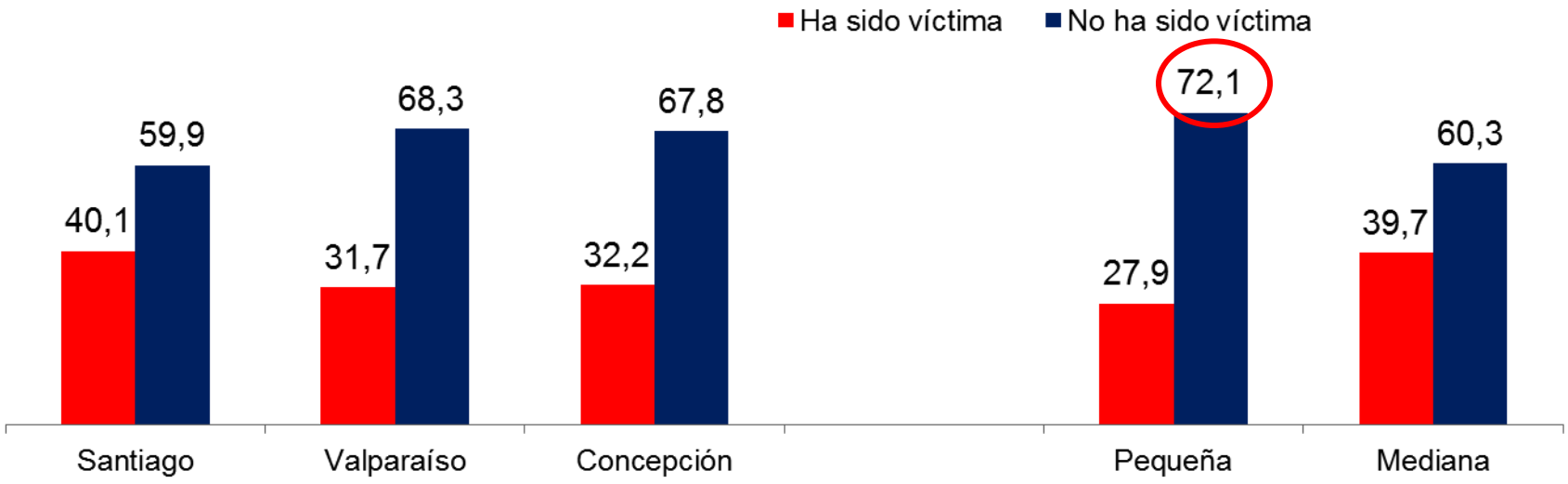
Han sido víctima?

Base: 612 casos

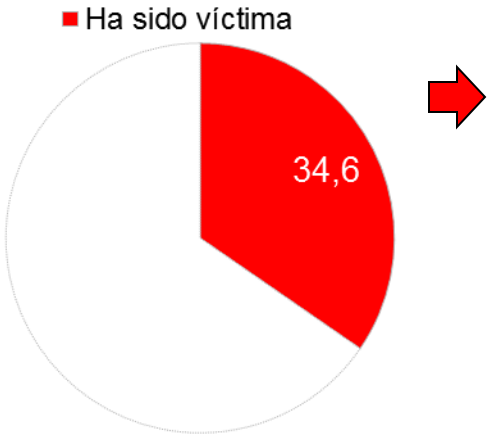


CIUDAD

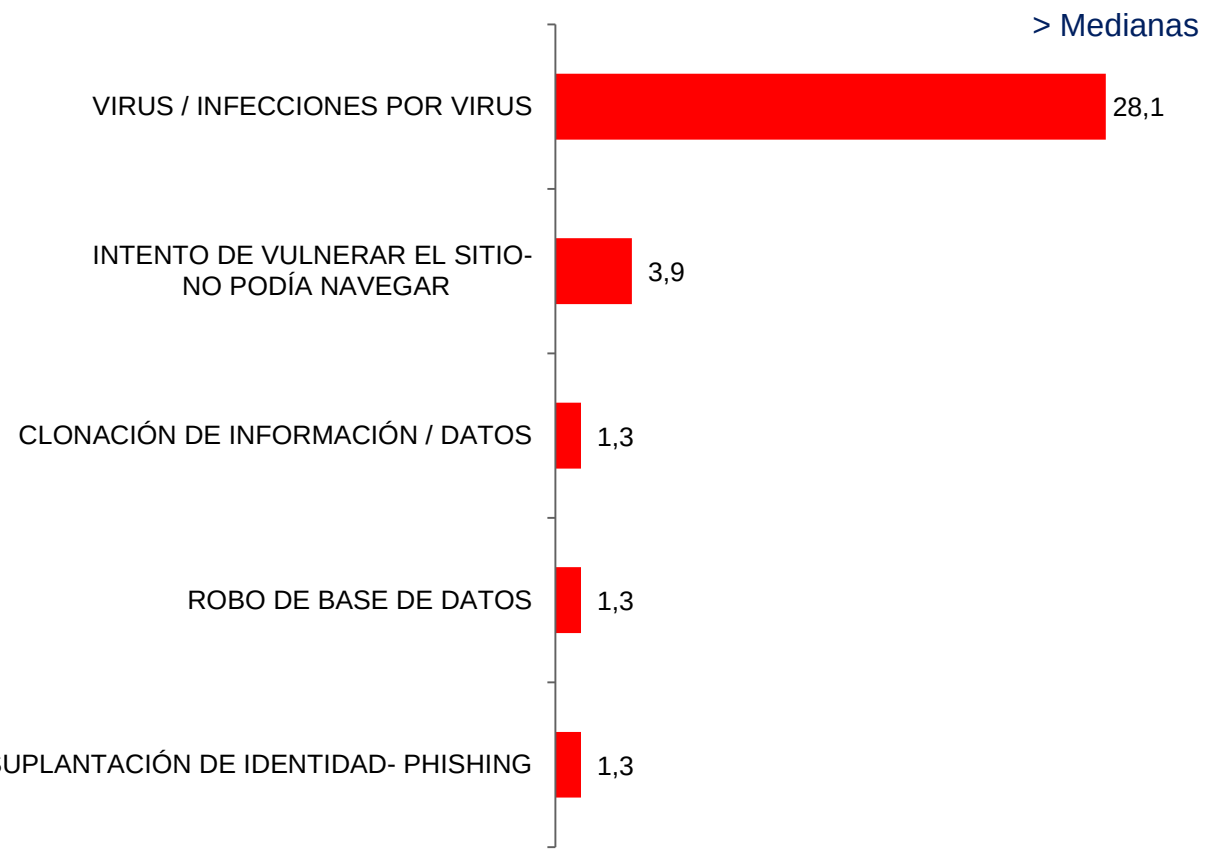
TAMAÑO EMPRESA



Incidentes experimentados

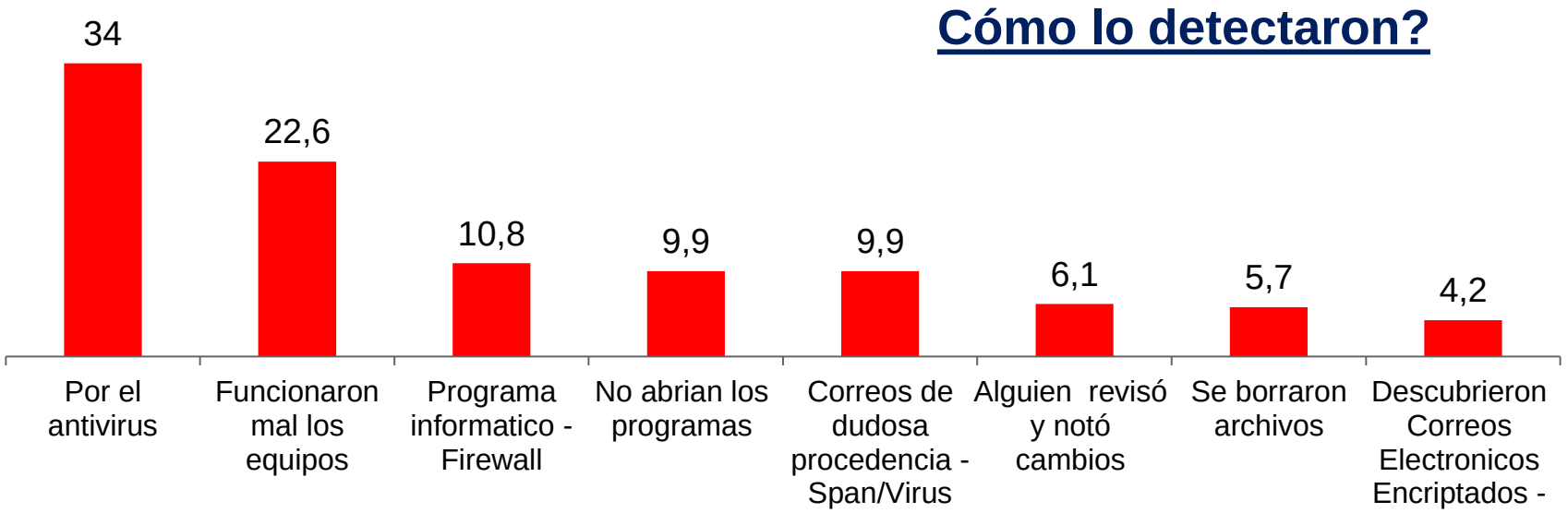


Base: 612 casos



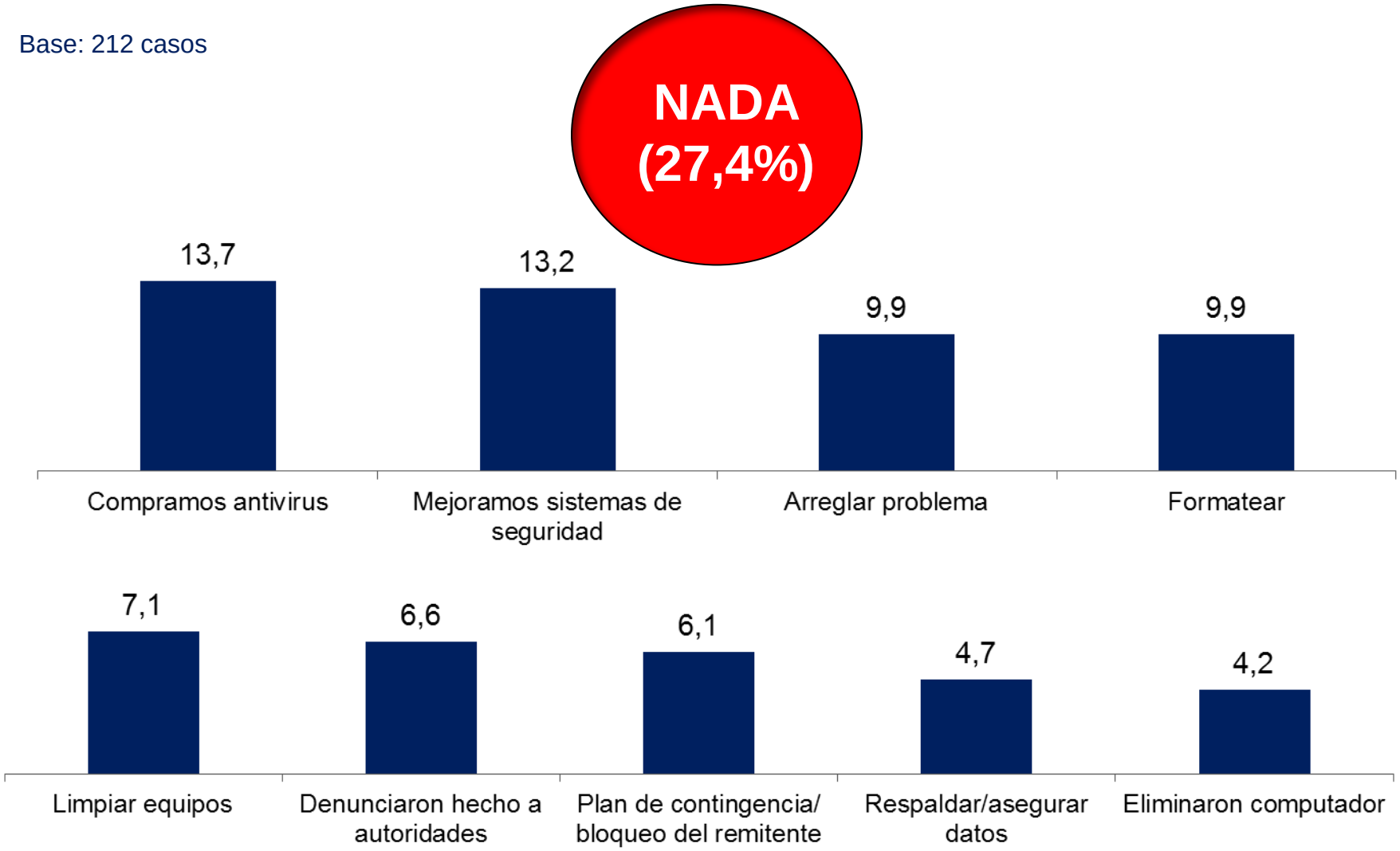
¿Cómo detectaron?

Base: 212 casos



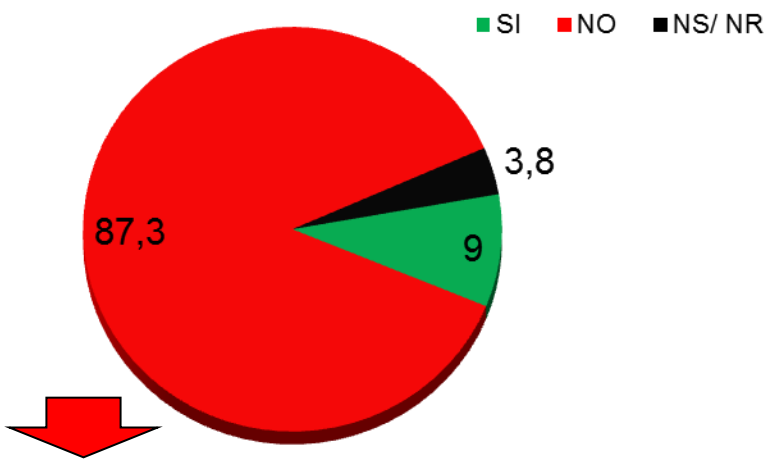
¿Qué hicieron en esa ocasión?

Base: 212 casos



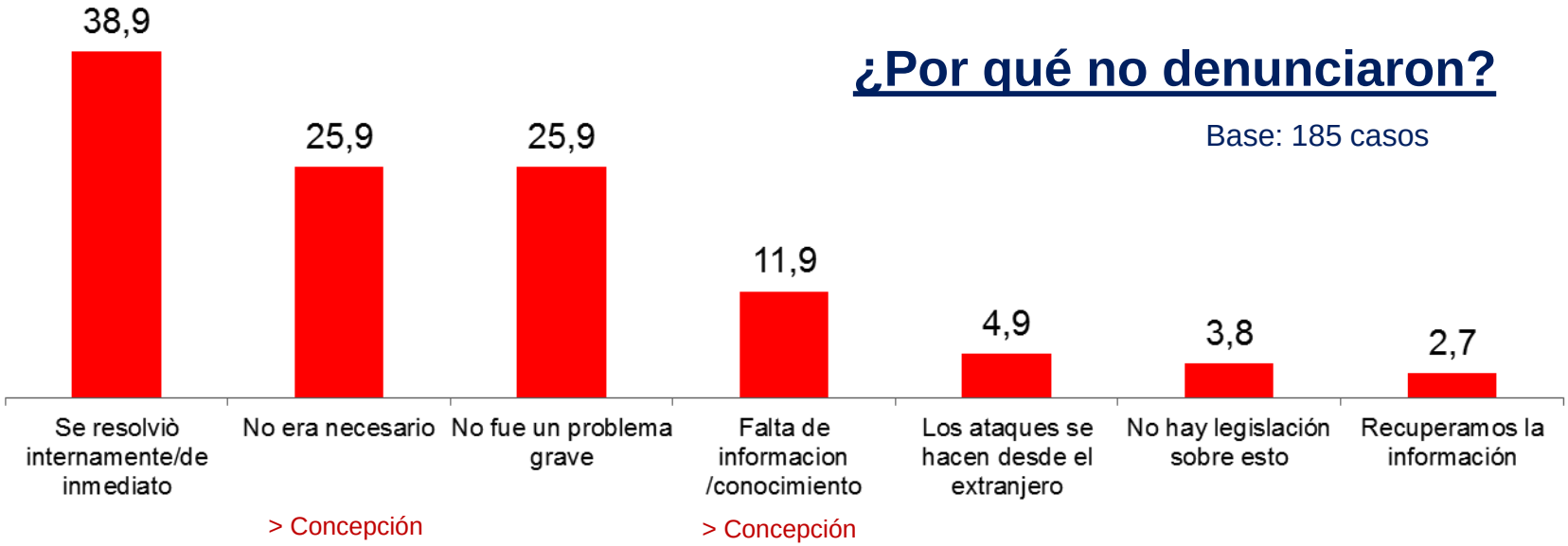
¿Denunciaron los hechos?

Base: 212 casos



¿Por qué no denunciaron?

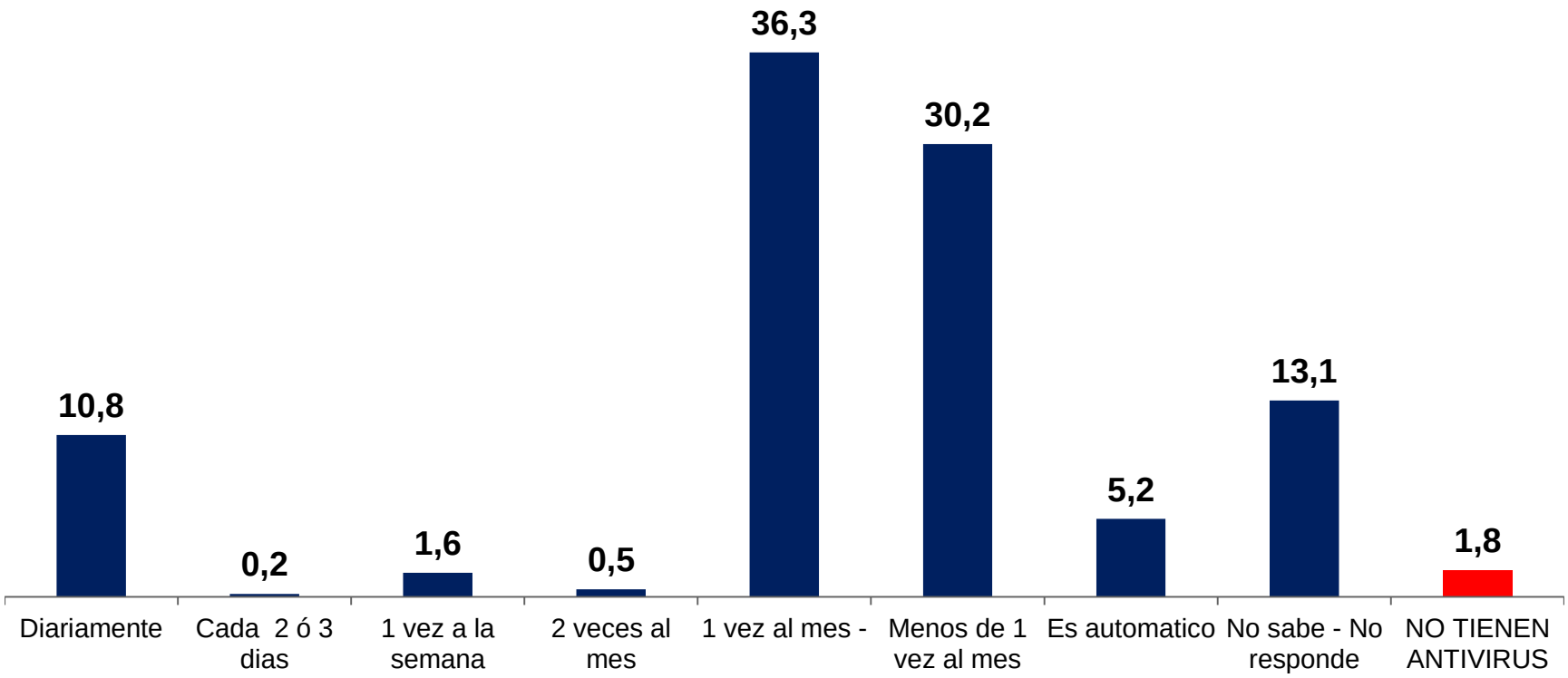
Base: 185 casos



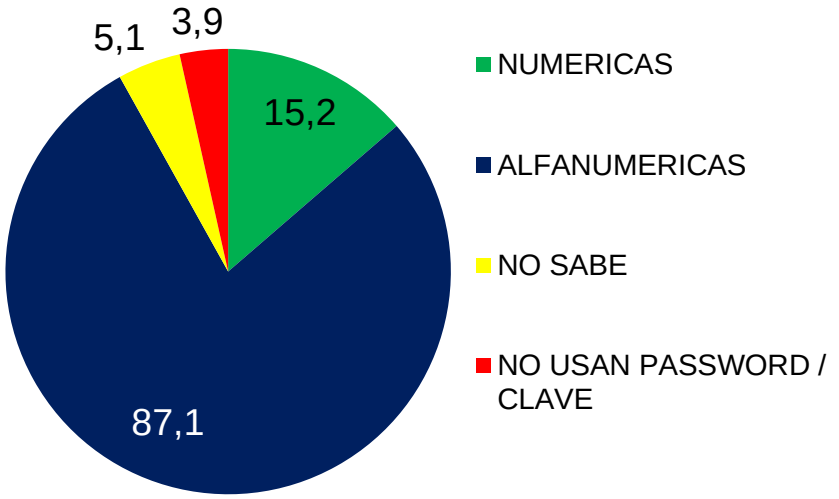
Antivirus y Claves de Acceso

Frecuencia de actualización de antivirus

Base: 612 casos

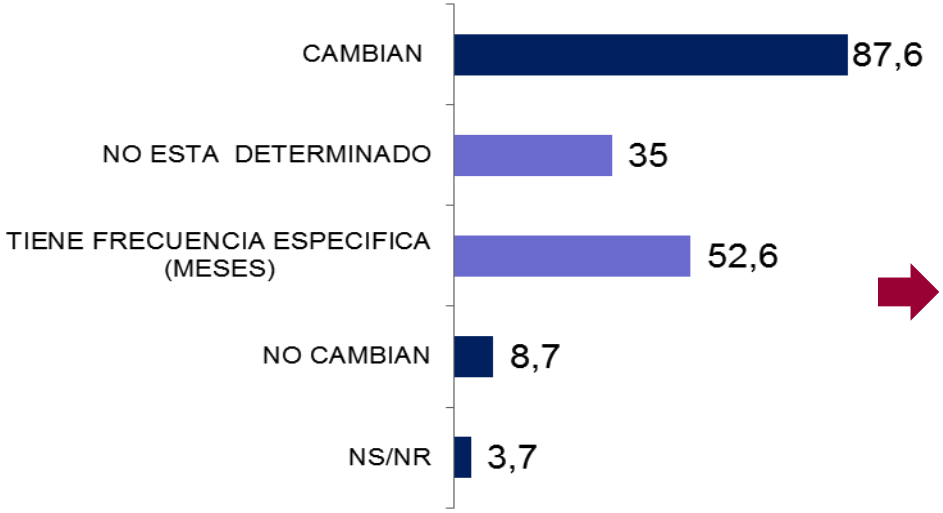


Uso de password – claves



Base: 612 casos

Frecuencia de cambio



Base: 588 casos

Promedio
Cada 5 meses

OBSERVATORIO DE COMERCIO ILÍCITO
CÁMARA NACIONAL DE COMERCIO, SERVICIOS Y TURISMO DE CHILE

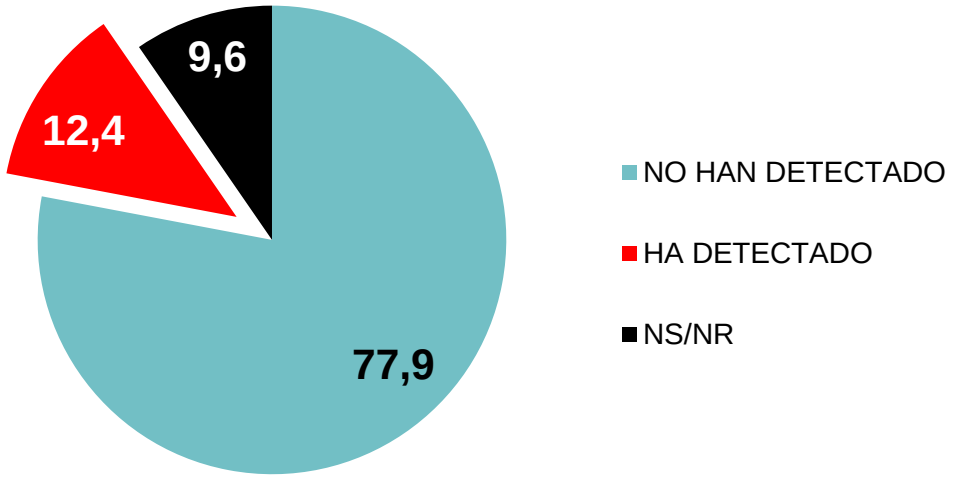
Microsoft

CNC La Cámara de Chile

Uso de Softwares sin Licencia

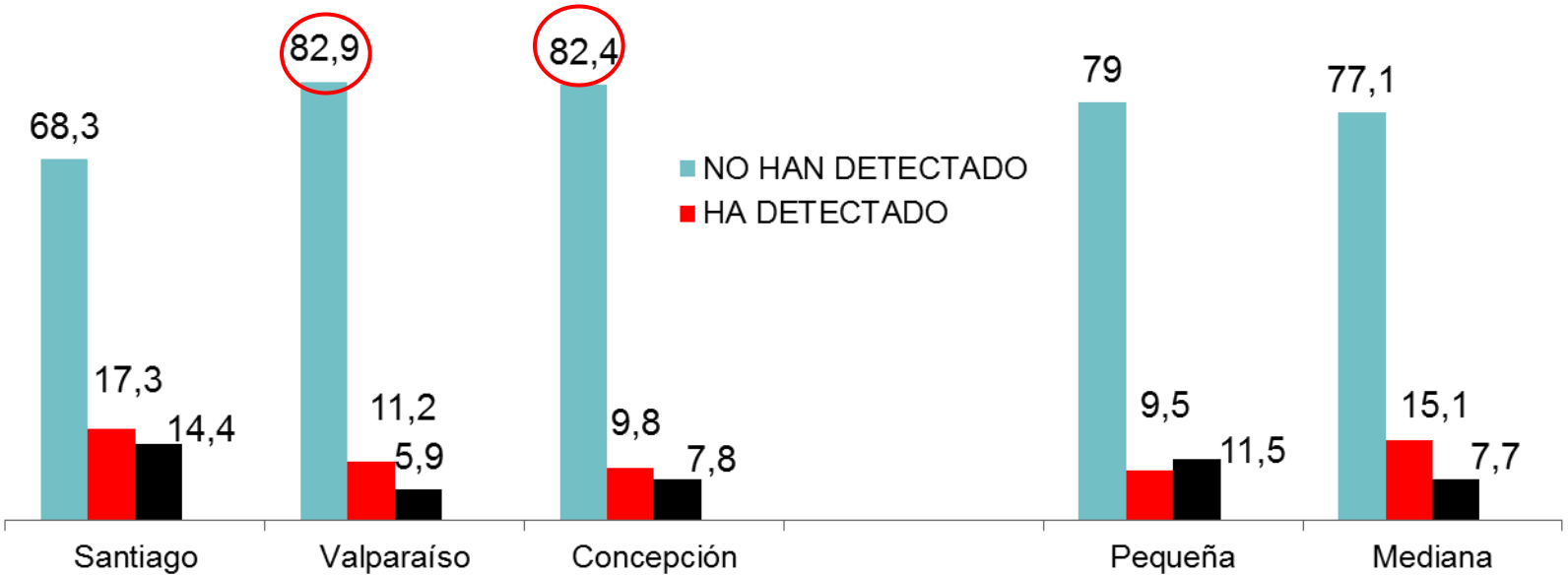
Han detectado Software sin licencia

Base: 612 casos



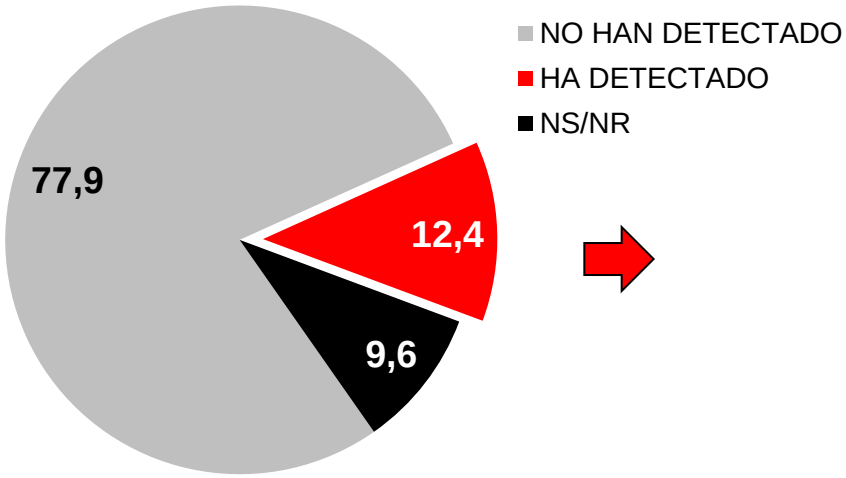
Ciudad

Tamaño de empresa

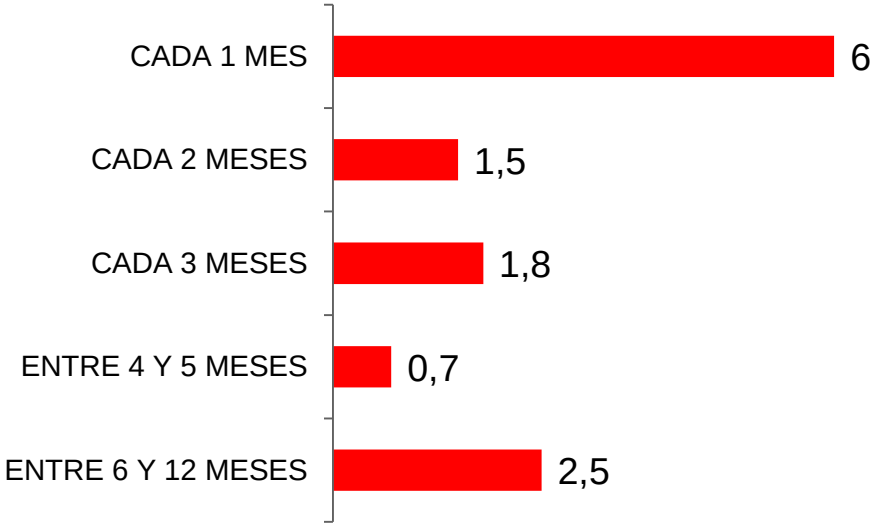


¿Con qué frecuencia detectan uso de Software sin licencia?

Base: 612 casos



Frecuencia detección (MESES)



Frecuencia promedio

	Total	Santiago	Valparaíso	Concepción	Pequeña	Mediana
PROMEDIO	3,092	3,771	2	3,105	2,625	3,308

¿Cómo detectan / evitan el uso de software sin licencia?

¿Cómo detectan?

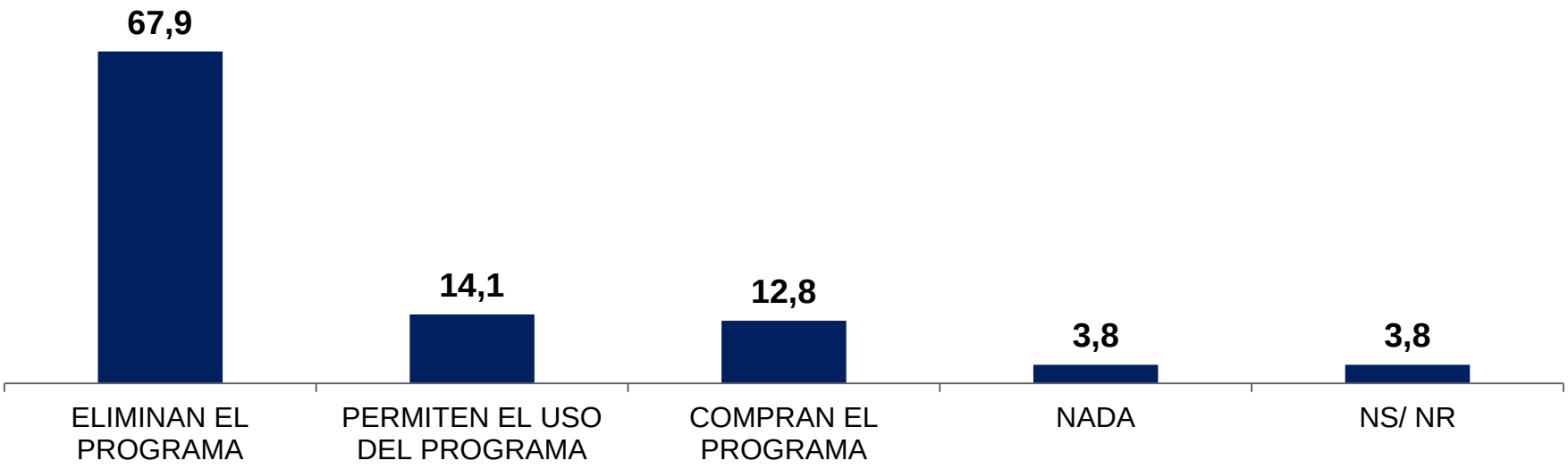
Base: 78 casos

¿Cómo evitan?

Base: 78 casos

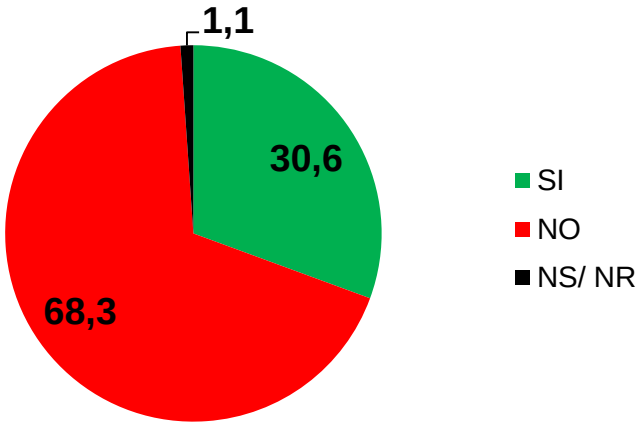
¿Qué hacen cuando detectan el uso de Software sin licencia?

Base: 78 casos

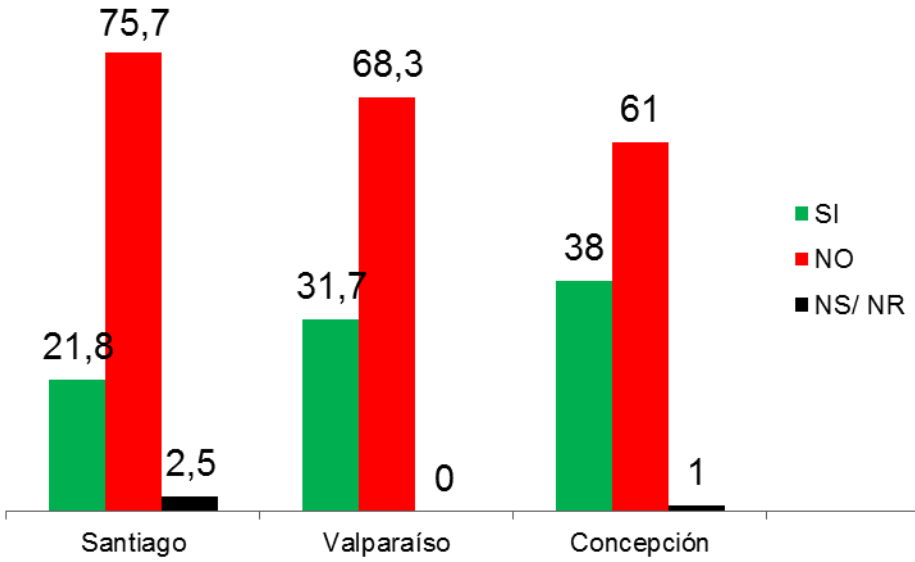


¿Hay libertad para bajar música o videos gratis?

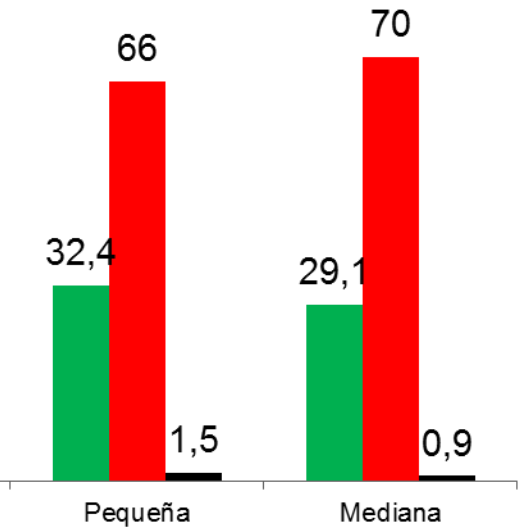
Base: 612 casos



Ciudad

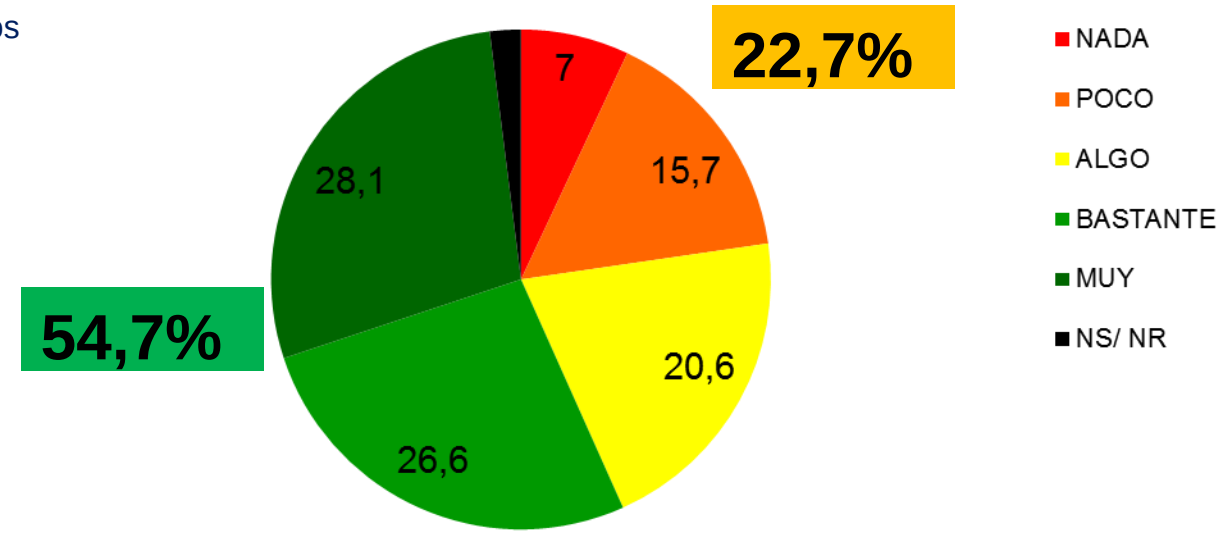


Tamaño de empresa



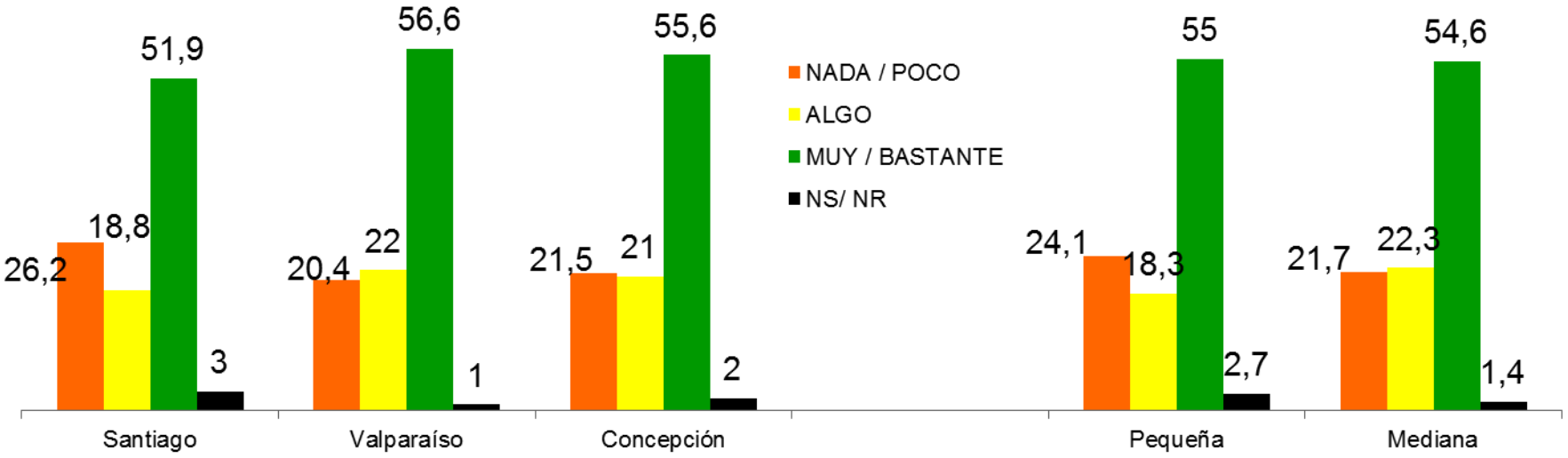
Consciencia sobre peligros por bajar programas gratis de la web

Base: 612 casos



Ciudad

Tamaño de empresa



OBSERVATORIO DE COMERCIO ILÍCITO
CÁMARA NACIONAL DE COMERCIO, SERVICIOS Y TURISMO DE CHILE

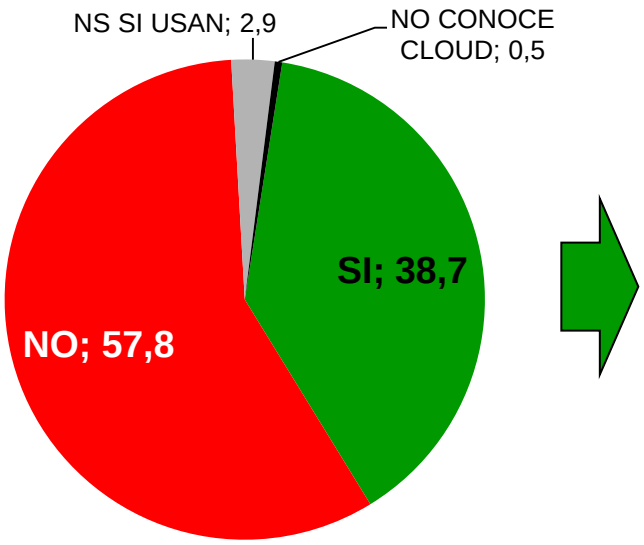
Microsoft

CNC La Cámara de Chile

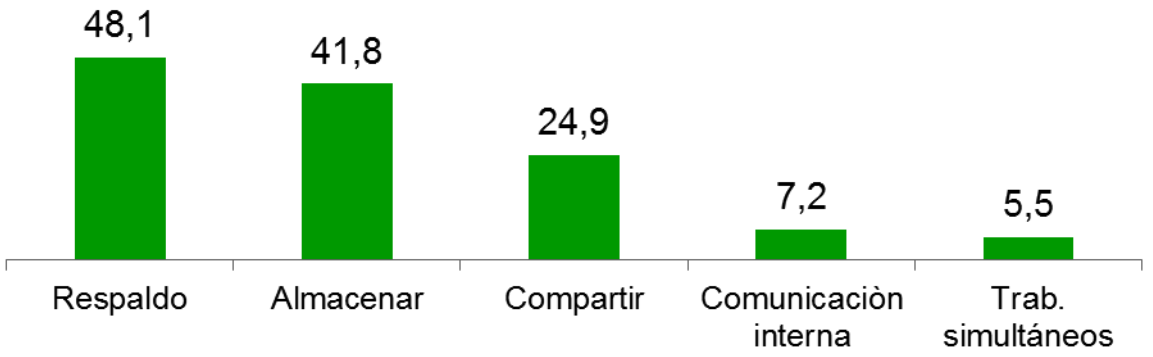
Información sobre Cloud

¿Utilizan Cloud?

Base: 612 casos

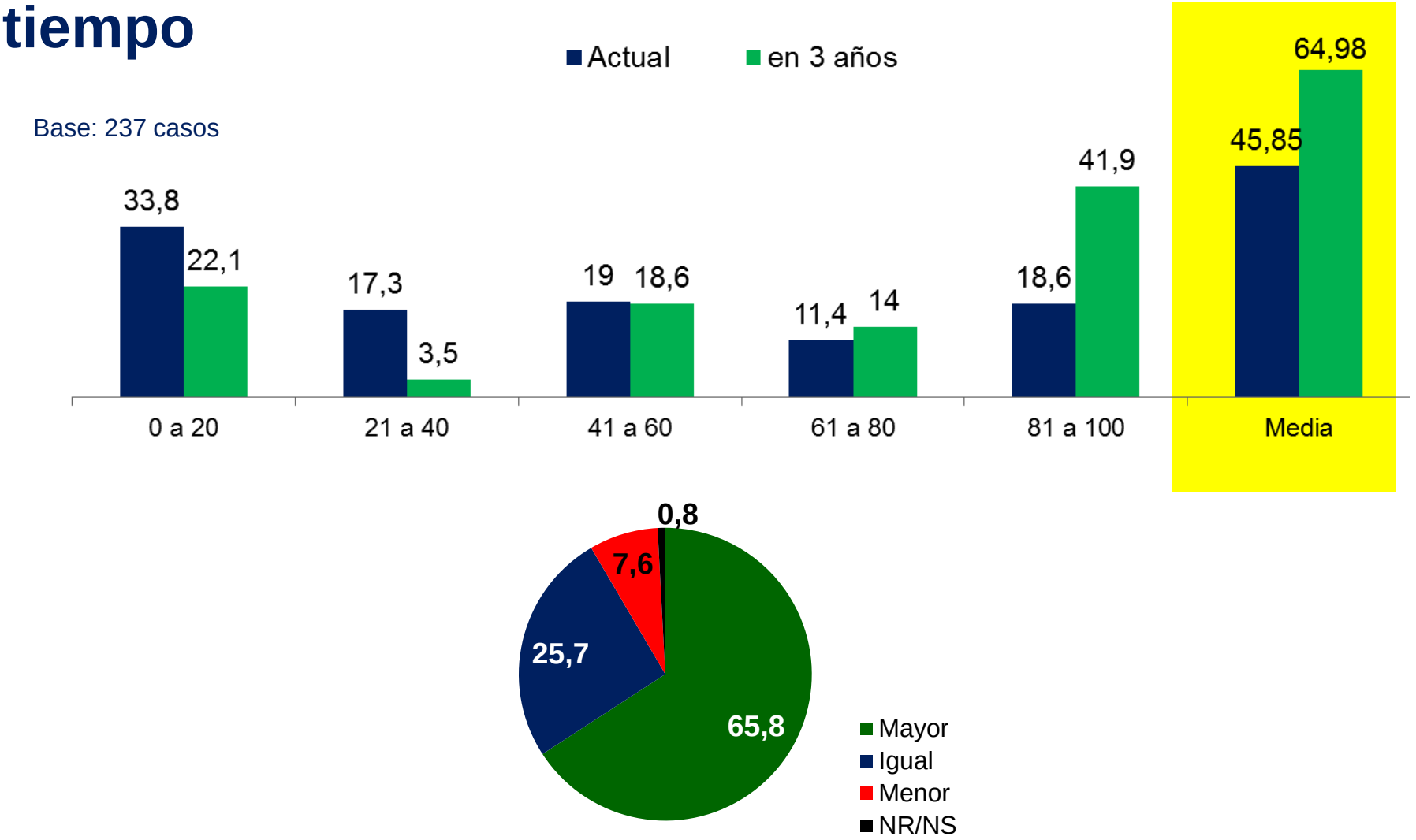


¿Para qué lo usan?



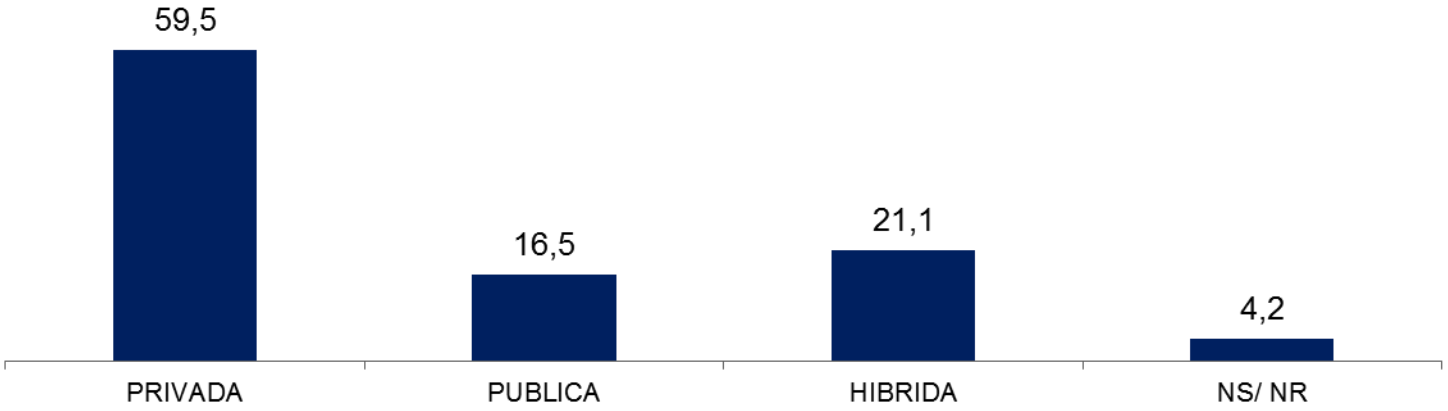
Base: 237 casos

% Operaciones atendidas por Cloud en el tiempo

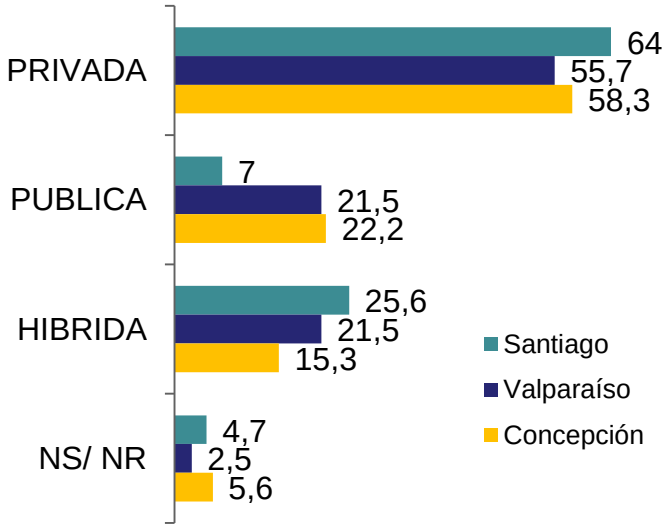


Tipo de Nube utilizada

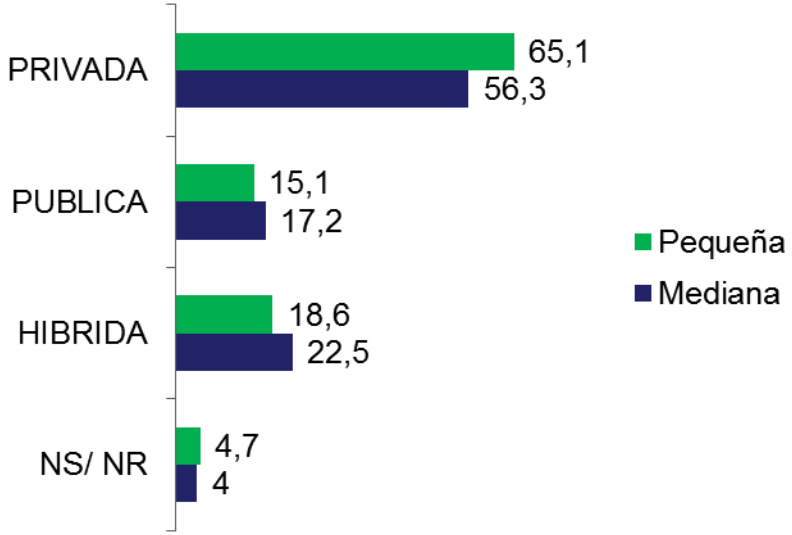
Base: 237 casos



Ciudad

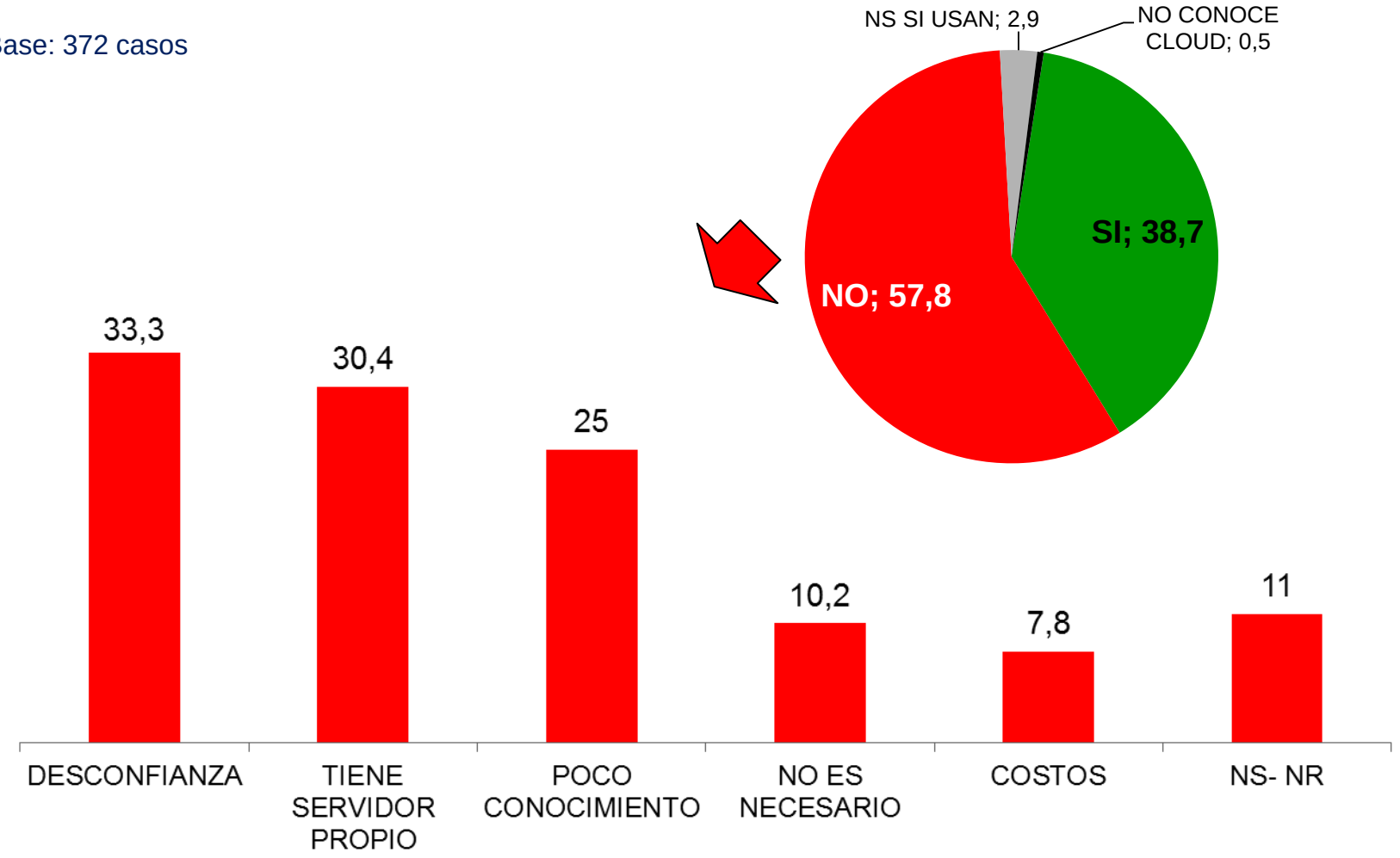


Tamaño de empresa



¿Por qué no usa la Nube pública?

Base: 372 casos



OBSERVATORIO DE COMERCIO ILÍCITO
CÁMARA NACIONAL DE COMERCIO, SERVICIOS Y TURISMO DE CHILE

Microsoft

CNC La Cámara de Chile

Conclusiones

OBSERVATORIO DE COMERCIO ILÍCITO
CÁMARA NACIONAL DE COMERCIO, SERVICIOS Y TURISMO DE CHILE

Microsoft

CNC La Cámara de Chile

La Ciberseguridad es una preocupación de todos

91%
de las compañías admiten haber sido víctimas de un ciberataque en 2015.

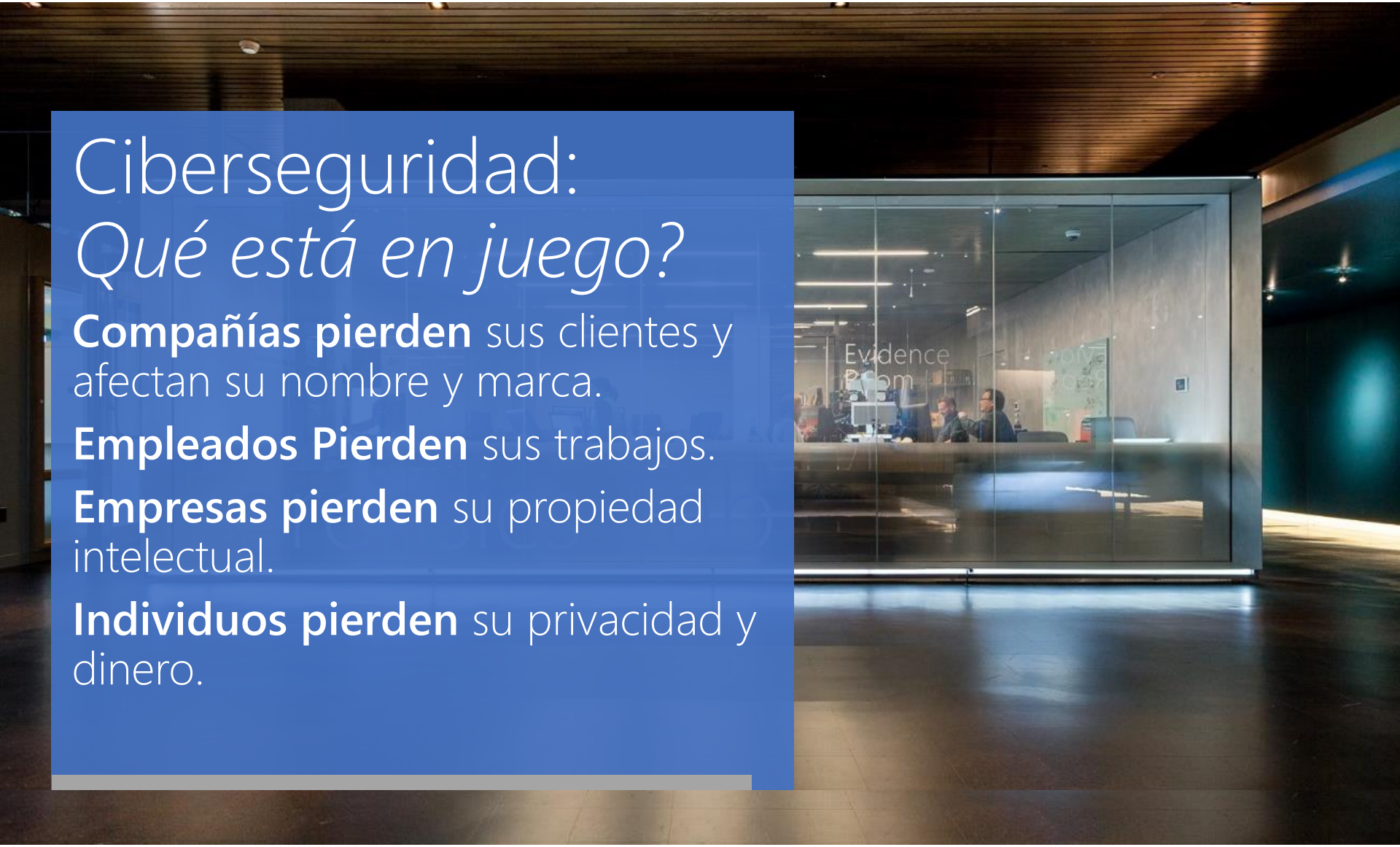
3B
Es el costo económico estimado, que va a provenir de la industria al cibercrimen en el 2020.

556M
víctimas anuales del cibercrimen

$400.000M
anuales les cuestan los ciberataques a las empresas

$160M
De registros de información personal filtrada dentro de los 8 mayores ataques cibernéticos del 2015.

140+
Tiene promedio entre una infección y su detección



Ciberseguridad: *Qué está en juego?*

Compañías pierden sus clientes y afectan su nombre y marca.

Empleados Pierden sus trabajos.

Empresas pierden su propiedad intelectual.

Individuos pierden su privacidad y dinero.

Estudios

Falsificación de Software y Malware

1 de cada 3

Software falsificado contiene Malware

0.79

Correlación entre el software sin licencia y las amenazas de seguridad

+60%

Posibilidad de encontrar malware en un equipo comprado con software pirata

País	Tasa Software sin Licencia	Tasa de Malware
Argentina	69	25
Brazil	50	31
Chile	59	22
Colombia	52	29
Dominican Republic	75	30
Ecuador	68	35
Guatemala	79	22
Mexico	54	31
Peru	65	37
Uruguay	68	19
Venezuela	88	32

Nivel de Madurez en Ciberseguridad

.cl

Chile

Política y estrategia

Cultura y sociedad

Educación

Marcos legales

Tecnología

El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen la política de seguridad cibernética a nivel gubernamental. Si bien el país no ha emitido una estrategia nacional de seguridad cibernética, la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y las partes interesadas pertinentes regularmente analizan los activos y vulnerabilidades de la Infraestructura Crítica Nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control. Uno de los principales desafíos de Chile de cara al futuro es el fortalecimiento de su capacidad de respuesta a incidentes: el CSIRT-CL que se encuentra en funcionamiento desde 2004 ofrece respuesta a incidentes para los sitios web del gobierno pero no está institucionalizado formalmente a nivel nacional para abordar todo tipo de violaciones.

Chile ha establecido un marco jurídico global para hacer frente a los delitos cibernéticos. El Decreto Supremo nº 1299 describe las normas y define los roles para el manejo de la delincuencia cibernética, la Ley nº 19.223 introduce los delitos informáticos al Código Penal y la Ley nº 19.628 cubre la privacidad y protección de datos. Aunque el sector privado no está obligado por ley a divulgar las violaciones, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a incidentes cibernéticos. De acuerdo con las autoridades de Chile, la suplantación de identidad (phishing), malware y piratería informática son los tipos más frecuentes de ataques cibernéticos en el país. El Departamento de Investigación de Organizaciones Criminales (OS-9) y el Laboratorio de Criminalística de los Carabineros (LABOCAR), la policía nacional de Chile, llevan a cabo investigaciones y análisis forense digital respectivamente. Estas unidades han detenido con éxito numerosos criminales cibernéticos en los últimos años. Por último, los tribunales tienen una capacidad adecuada para manejar evidencia electrónica.

La mentalidad de seguridad cibernética es inconsistente en la sociedad chilena. En 2013, para crear conciencia, el Ministerio de Educación inició la campaña de Internet Segura para educar a los jóvenes sobre la privacidad y el uso seguro de Internet. También está en marcha una campaña, llamada Consumidor Digital, para que los ciudadanos tengan cuidado de los riesgos del comercio electrónico y para que entiendan sus derechos como consumidores. La Universidad de Chile ofrece títulos avanzados en seguridad cibernética y también están disponibles diversos cursos en línea y capacitación para empleados. Comparativamente, el sector privado se ha vuelto cada vez más consciente de los riesgos de seguridad cibernética y ha puesto en marcha planes para abordarlos.

POBLACIÓN TOTAL DEL PAÍS	17.762.647
Abonos a teléfonos celulares	23.683.351
Personas con acceso a Internet	12.789.105

Penetración de Internet

72%

STARTUP · FORMATIVE · ESTABLISHED · STRATEGIC · DYNAMIC

Tendencias

- **1/3 empresas ha sido víctima de un incidente de seguridad.**
- Coincide con **Kaspersky (2015): 91%** de las empresas encuestadas fue víctima de un delito informático".
- Incidente fue detectado **después** de ocurrido.
- **McKinsey (2015)** "Las empresas demoran más de **200 días** en detectar incidentes de seguridad".
- En cuanto a las acciones tomadas, el **27,4% no hizo NADA**.
- Quienes si realizaron alguna acción, mencionan que compraron antivirus, lo que representa al 13,7%
- Según **Kaspersky**: "**A pesar del aumento de los delitos informáticos, solo 43% utiliza sistemas preventivos de ataques y el 15% desconoce sistemas de seguridad contra malware avanzado".**

Qué hacer?

- 87,3% no denuncia
- Ley de Delitos Informáticos 19.223, es de 1993,
- Adopción Convenio de Budapest de 2001.

Medidas Preventivas:

- Alto nivel de uso de Antivirus (98,2%)
- Alto nivel de uso de Claves de acceso (96,1%)
- Alto nivel de restricción para bajar música o videos gratis (68,3%)

Las empresas que usan claves de acceso:

- Tienen un Encargado de IT para el control de ellas (52%):

  Políticas/procesos claros son críticos para proteger el entorno digital de una organización.

Nivel de Consciencia Medio de los Riegos

- **54,7%** consciente de los peligros.
- **43,3%** Nada o Algo consciente.
- **2015 McKinsey** concluye que la ciberseguridad paso a ser un asunto propio de los directores de las empresas y no de los gerentes de TI.

Uso de la Nube

- El 38,7% Usa la Nube: Respaldar, Almacenar y Compartir datos.
- 33% no la usa por Desconfianza.

- Percepción de aumento de uso de la Nube: 64,98% aumenta a 3 años.

- Estudio Chile 4.0 de Fundación Chile (2016):
- Riesgos asociados al uso de la Nube: Seguridad 68% y Principales riesgos a la Seguridad provienen de empleados antiguos y actuales.

Enfoque Integral

- Actualización de TI
- Educación
- Alianzas Público/Privadas
- Actualización Legal

OBSERVATORIO DE COMERCIO ILÍCITO
CÁMARA NACIONAL DE COMERCIO, SERVICIOS Y TURISMO DE CHILE

Microsoft

CNC La Cámara de Chile

Muchas Gracias!

www.observatoriocomercioilicito.cl

@OCI Chile

informaciones@observatoriocomercioilicito.cl