AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Desafíos de la ciberseguridad en los municipios de Chile

Radiografía a sus procesos y normas en 2024

Presentación

Desde el 2022 que AMUCH ha liderado el proceso de transformación digital en los municipios mediante la creación, del **Programa Nacional de Impulso a la Transformación Digital a nivel local.**

A dos años de su inicio, este programa ha impulsado más de 17 iniciativas para fortalecer la capacidad digital de los municipios, incluyendo capacitaciones, seminarios, concursos de buenas prácticas, cursos para funcionarios municipales y encuentros con empresas que promueven la transformación digital y la ciberseguridad en el ámbito municipal.

La primera etapa de la **Ley de Transformación Digital** está actualmente en marcha en los municipios del país, marcando un hito en la modernización y fortalecimiento de su infraestructura digital. En paralelo, la promulgación de leyes clave, como **la Ley de Protección de Datos Personales**, que establece la Agencia de Protección de Datos Personales, y la **Ley Marco de Ciberseguridad**, han posicionado a Chile como pionero en la región en términos de desarrollo legislativo en el ámbito digital.

https://www.tdmunicipal.cl/

Este marco legal robusto ha impulsado a Chile a ascender 30 posiciones en el ranking mundial de ciberseguridad de 2024, situándolo en el puesto 25 global y segundo en América Latina, según el índice de Nacional Cyber Security Index (NCSI).

La Ley N°21663 Marco Ciberseguridad define la ciberseguridad como la **preservación de la confidencialidad, integridad, disponibilidad y resiliencia de redes y sistemas informáticos, con el fin de proteger a personas, organizaciones y naciones de posibles incidentes.** Sin embargo, como se detallará más adelante, aún persisten importantes brechas y desafíos específicos en el ámbito municipal que requieren atención y trabajo conjunto.

¿Cómo obtuvimos los datos?

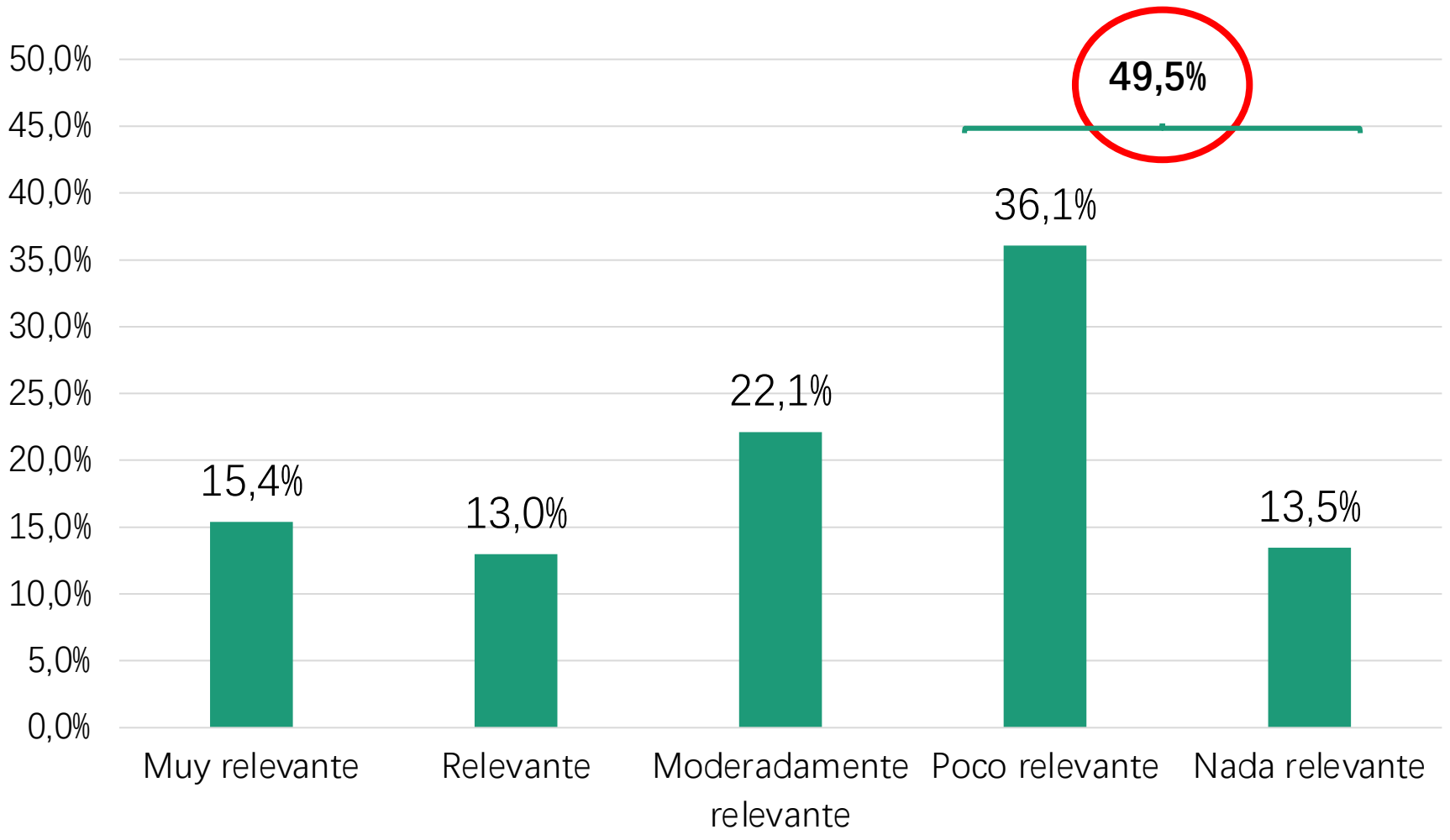
Cuestionario telefónico y/o auto aplicado a los Coordinadores(as) de Transformación Digital o encargados(as) del Área de Información, Tecnología e Informática en cada municipio.

Grupo de comunas	Formulario online	
	Representatividad	N°
Grandes comunas metropolitanas con alto y/o medio desarrollo	66,0%	31
Comunas mayores con desarrollo medio	73,0%	27
Comunas urbanas medianas con desarrollo medio	60,7%	34
Comunas semiurbanas y rurales con desarrollo medio	54,2%	52
Comunas semiurbanas y rurales con bajo desarrollo	58,7%	64
Nacional	**60,3%**	**208**

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Opinión sobre el nivel de relevancia que otorgan alcaldes(as) y directivos a la ciberseguridad

Qué tan relevante es para las autoridades del municipio la promoción de la ciberseguridad



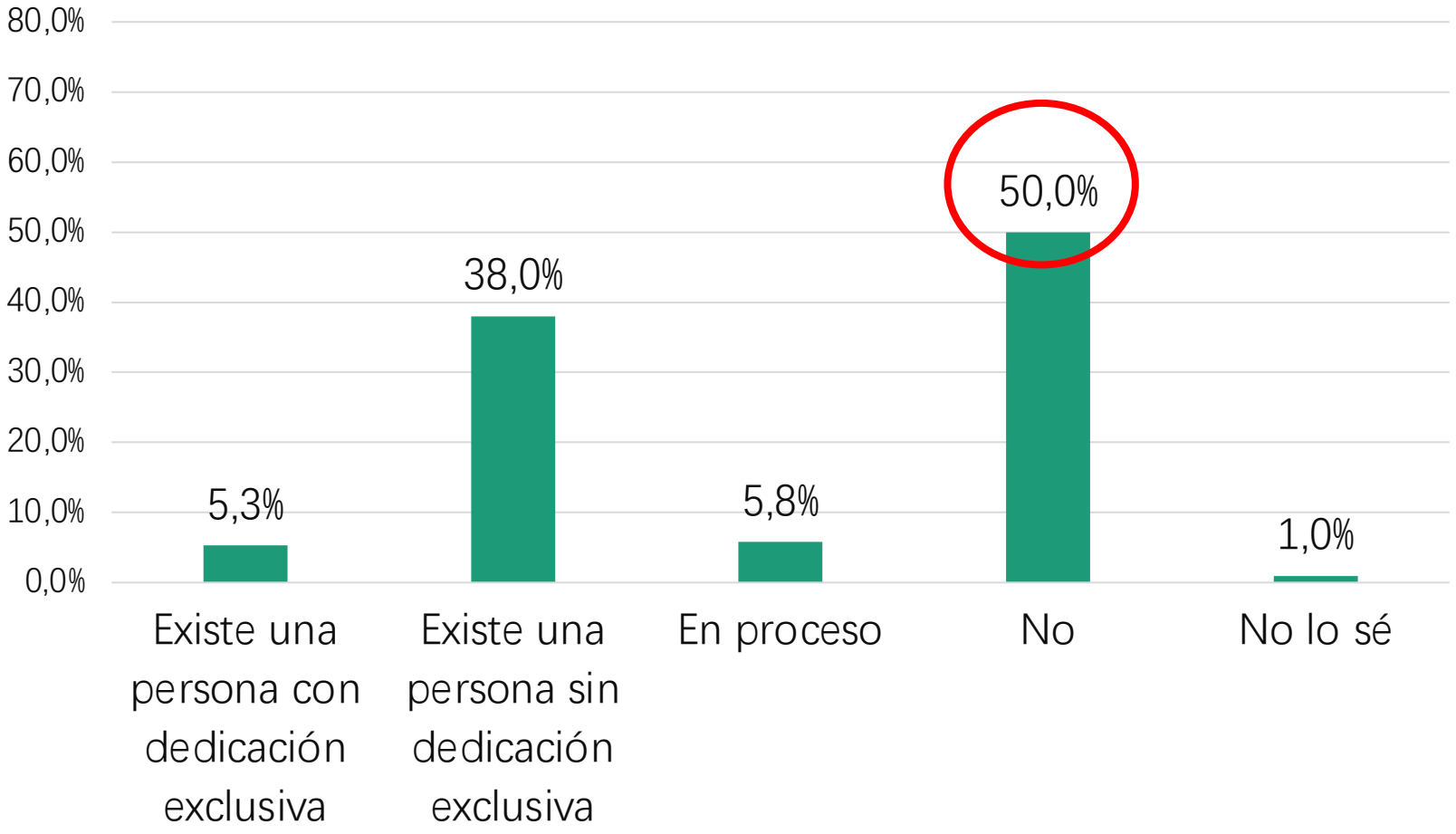
Un 49,5% de coordinadores de TD y/o encargados(as) de informática consideran que los tomadores de decisión consideran poco o nada relevante la ciberseguridad.

Sólo un 28,4% cree que es considerado como un tema muy relevante o relevante.

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Funcionario(a) municipal responsable de ciberseguridad o seguridad de la información

Con relación a la existencia de un funcionario(a) municipal responsable de ciberseguridad o seguridad de la información



- 5 de cada 10 municipalidades no tiene personal dedicado a pensar la ciberseguridad o seguridad de la información.
- Tendencia a externalizar servicios por baja capacidad institucional.

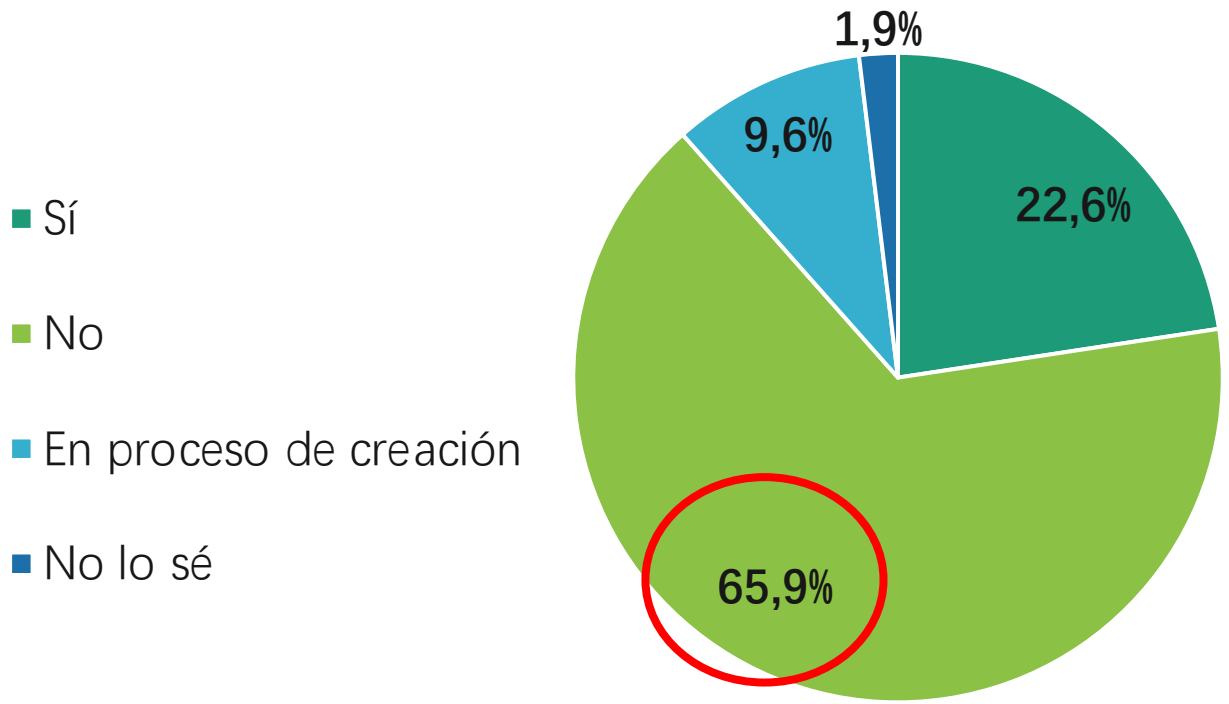
	Dedicación exclusiva	Sin dedicación exclusiva	En proceso	No
Grandes comunas metropolitanas con alto y/o medio desarrollo	12,9%	41,9%	6,5%	38,7%
Comunas mayores con desarrollo medio	7,4%	37,0%	7,4%	48,1%
Comunas urbanas medianas con desarrollo medio	5,9%	35,3%	5,9%	52,9%
Comunas semiurbanas y rurales con desarrollo medio	1,9%	40,4%	5,8%	48,1%
Comunas semiurbanas y rurales con bajo desarrollo	3,1%	35,9%	4,7%	56,3%

Tiende a existir un funcionario(a) municipal que cumple además de otras funciones el pensar en ciberseguridad y seguridad de la información ¿tiene capacidad de gestión el funcionar?

Escasa o nula capacidad de gestión

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

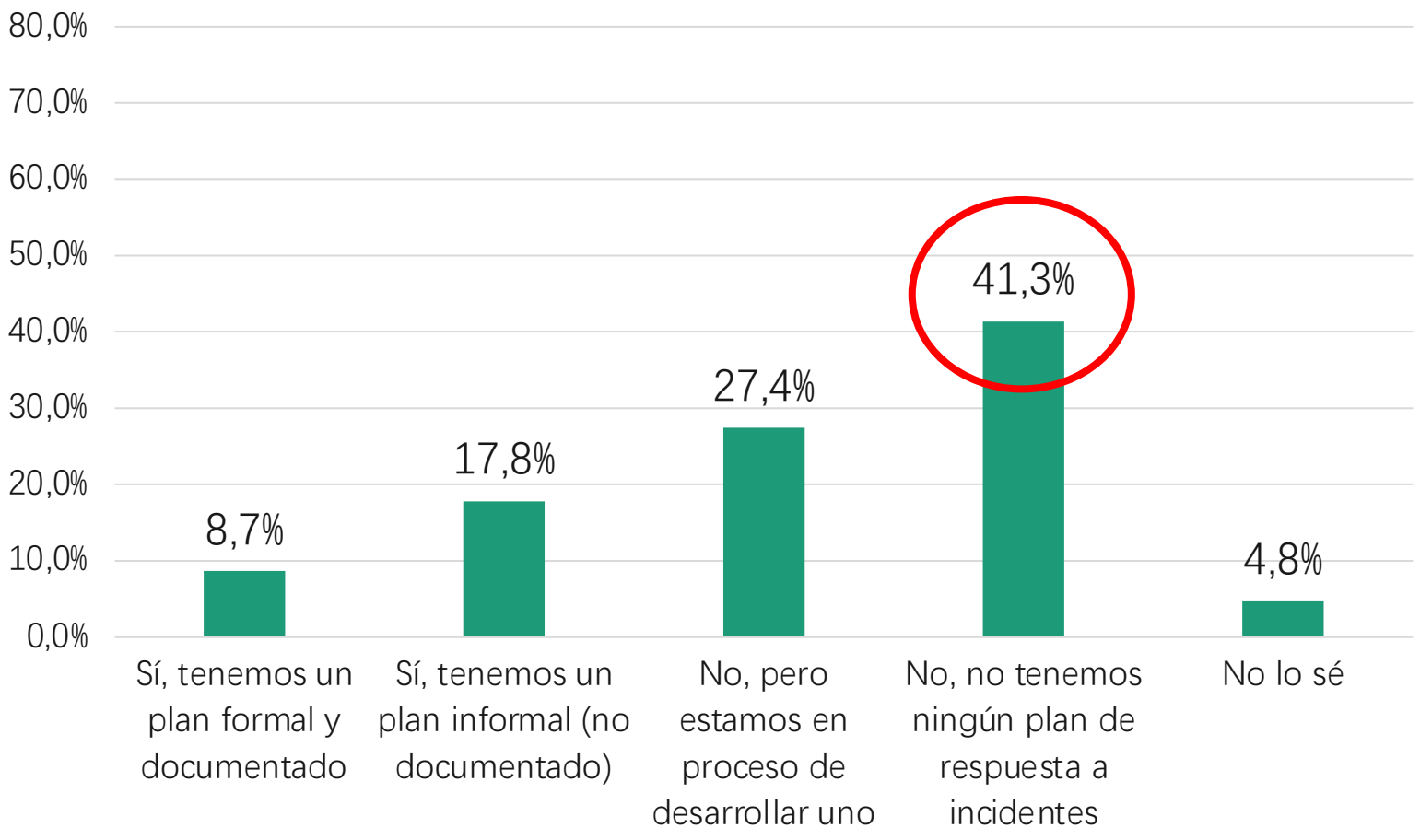
Comité de seguridad de la Información y planificación para responder a incidentes de ciberseguridad



6 de cada 10 municipios
No tienen un Comité de Seguridad

Un Comité de Seguridad es un órgano que coordina y supervisa las actividades relacionadas con la protección de la información y la ciberseguridad dentro de una institución, está compuesto por representantes de diversas áreas y su objetivo es garantizar la seguridad de los activos de información y el cumplimiento de las normativas.

¿Y un plan de respuesta a incidentes de ciberseguridad?



La Ley 21663 define un incidente de ciberseguridad **como cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información y los sistemas informáticos.**

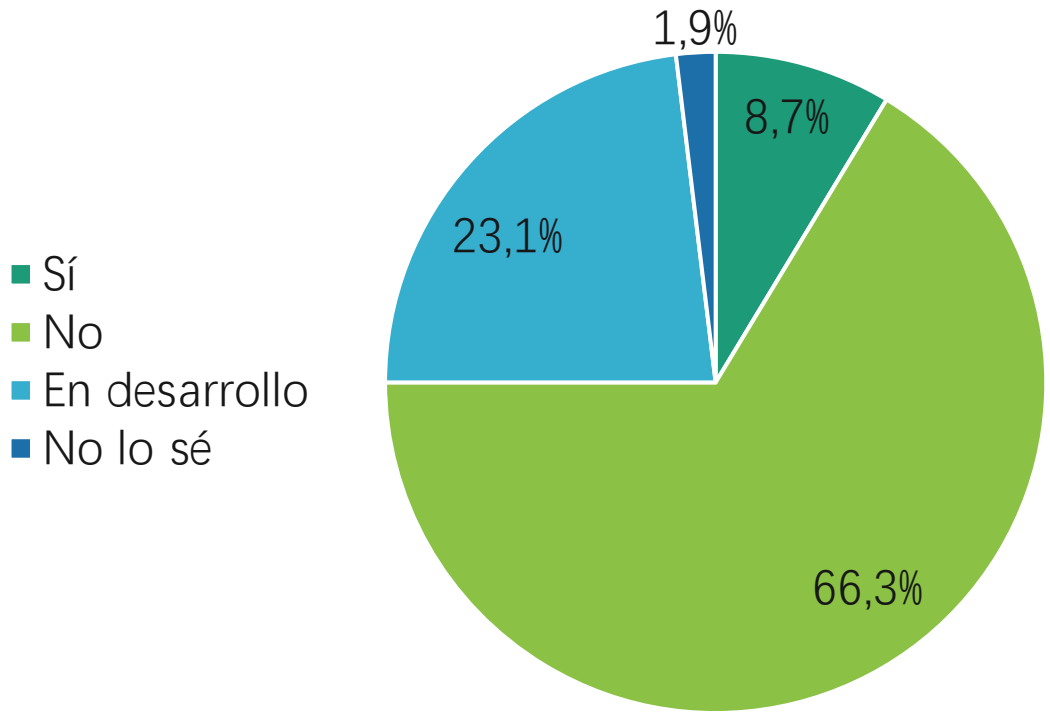
A nivel central se crea el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), encargado de prevenir, detectar, gestionar y responder a estos incidentes de manera rápida y efectiva, siguiendo procedimientos y políticas predefinidas para mitigar sus efectos.

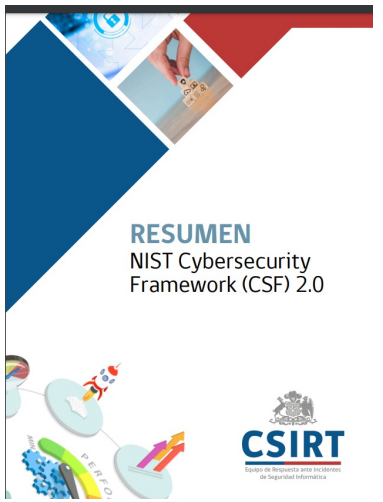
¿Y las municipalidades?

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Ciberseguridad: Manual para Funcionarios Municipales

De 135.970 funcionarios(as) municipales
81.402 no tienen acceso a este tipo de documentación.



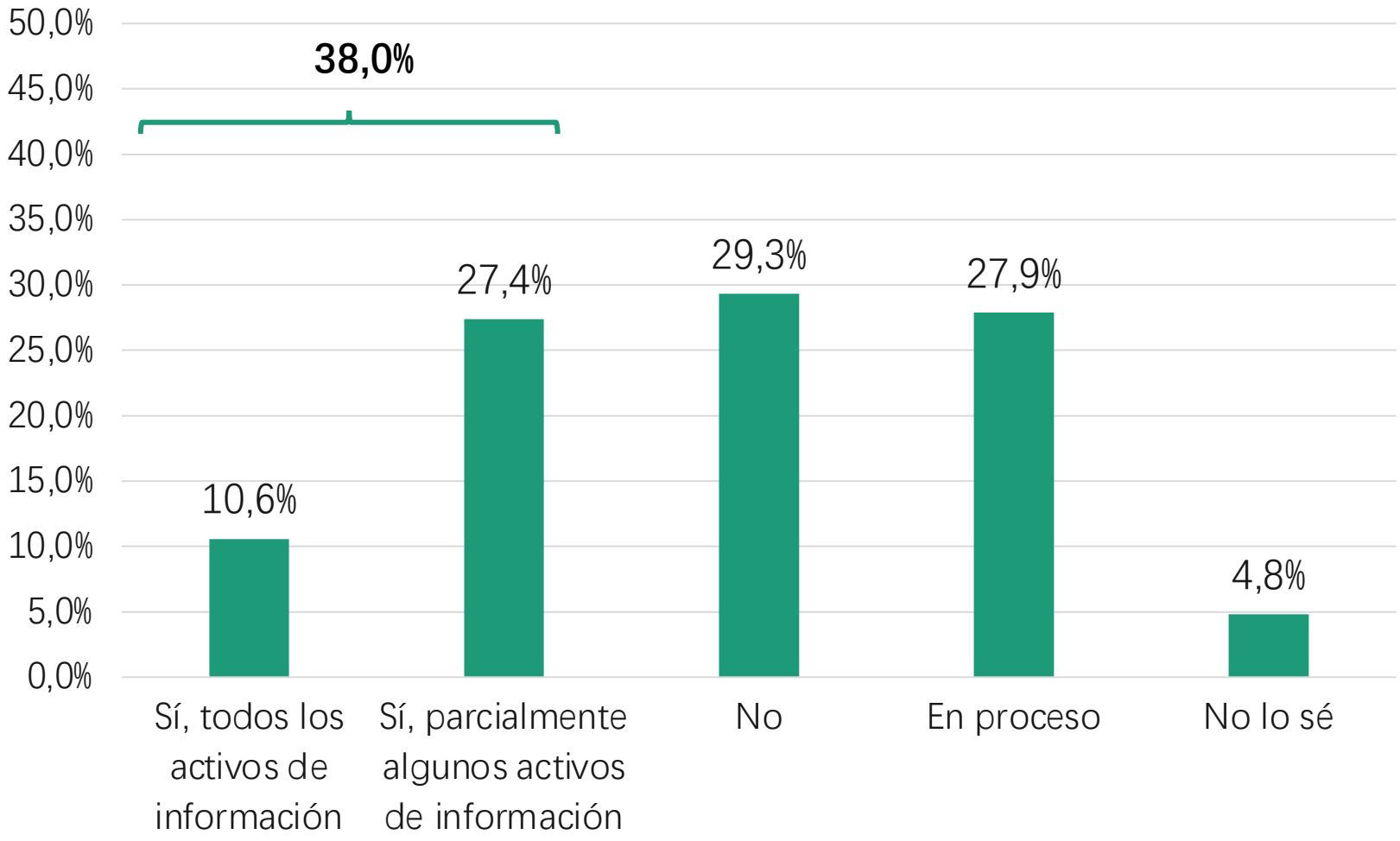


6 de cada 10 municipios
No tiene manual de ciberseguridad para funcionarios(as) municipales

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Identificación Activos de Información

La Ley 21663 Marco Ciberseguridad define activo informático como toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.



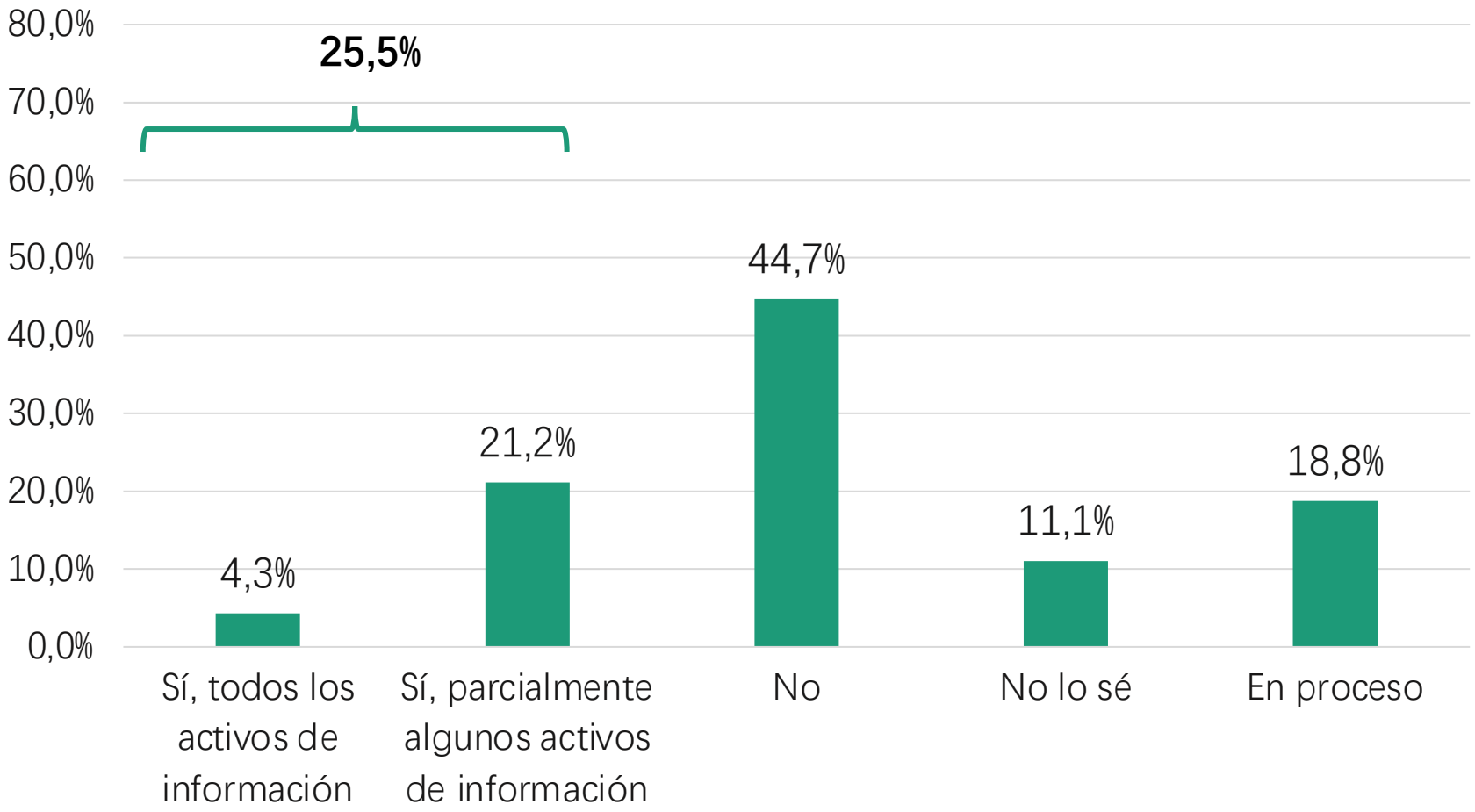
Las municipalidades como administraciones comunales son instituciones que crean y gestionan gran cantidad de datos e información para el cumplimiento de sus objetivos.

Sólo 1 de cada 10 municipalidades tiene identificados todos sus activos.

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

Análisis de riesgo de los activos de información

Análisis de riesgo de los activos de información



Para el análisis de los riesgos, es necesario tener identificado los activos de información.

El análisis de riesgo en ciberseguridad es esencial para identificar y priorizar amenazas, anticipar vulnerabilidades y tomar decisiones informadas sobre medidas de protección.

Un 44,7% no tiene análisis de riesgos y en contraste sólo un 25,5% tiene acciones.

AMUCH
ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

¿Cómo los municipios clasifican actualmente la información según criterios de seguridad?

Sí, tenemos un **procedimiento** que aplica para toda la información municipal	6,7%
Sí, tenemos un **procedimiento** que aplica para alguna información específica	10,6%
Sí, tenemos un **mecanismo q**ue aplica para toda la información municipal	5,3%
Sí, tenemos un **mecanismo** que aplica para alguna información específica	12,0%
No	**57,2%**
No lo sé	8,2%

El análisis de riesgo en ciberseguridad es esencial para identificar y priorizar amenazas, anticipar vulnerabilidades y tomar decisiones informadas sobre medidas de protección.

Un 57,2% no tiene procedimientos, mecanismos para clasificar sus activos de información según criterios de seguridad.

Son instituciones altamente vulnerables

AMUCH

ASOCIACIÓN DE MUNICIPALIDADES DE CHILE

www.amuch.cl