ESTUDIO SOBRE CIBERSEGURIDAD EN LAS IES MIEMBROS DE CUDI

CSIRT

ANTECEDENTES

Conscientes de la cada vez mayor relevancia de la ciberseguridad en el entorno actual, el CSIRT de CUDI decidió realizar un estudio para detectar la situación entre las IES miembros de CUDI.

OBJETIVO GENERAL

Entender cuáles son los problemas que enfrentan en su trabajo las IES miembros de CUDI así como los recursos con los que cuentan para solucionarlos. Ello con el fin de poder diseñar en el CSIRT de CUDI estrategias de apoyo que les sean útiles en el cambiante entorno de las TI.

METODOLOGÍA Y MUESTRA
Fase 1 cualitativa

SESIONES DE GRUPO

	CARACTERÍSTICAS Integrantes de las áreas de ciberseguridad y TI de las IES
1	Universidad de Guadalajara; Universidad Autónoma de Tamaulipas; Instituto Nacional de Astrofísica, Óptica y Electrónica; Universidad Autónoma de Ciudad Juárez; Universidad de Guanajuato; Universidad Autónoma de Chiapas; Colegio de Ingenieros en TIC del Estado de Guerrero
2	Universidad Nacional Autónoma de México; Universidad Autónoma Metropolitana; Instituto Politécnico Nacional; Universidad Autónoma de Nuevo León; Universidad Veracruzana; Universidad Autónoma de Yucatán
3	Instituto Tecnológico Autónomo de México; Universidad Iberoamericana CDMX; Comisión Nacional para el Conocimiento y Uso de la Biodiversidad

METODOLOGÍA Y MUESTRA
Fase 2 cuantitativa

Encuesta *on line* (170 entrevistas*) entre responsables de las áreas de ciberseguridad de las IES miembros de CUDI.

*Respondió el 85% de las instituciones invitadas a contestar el cuestionario.

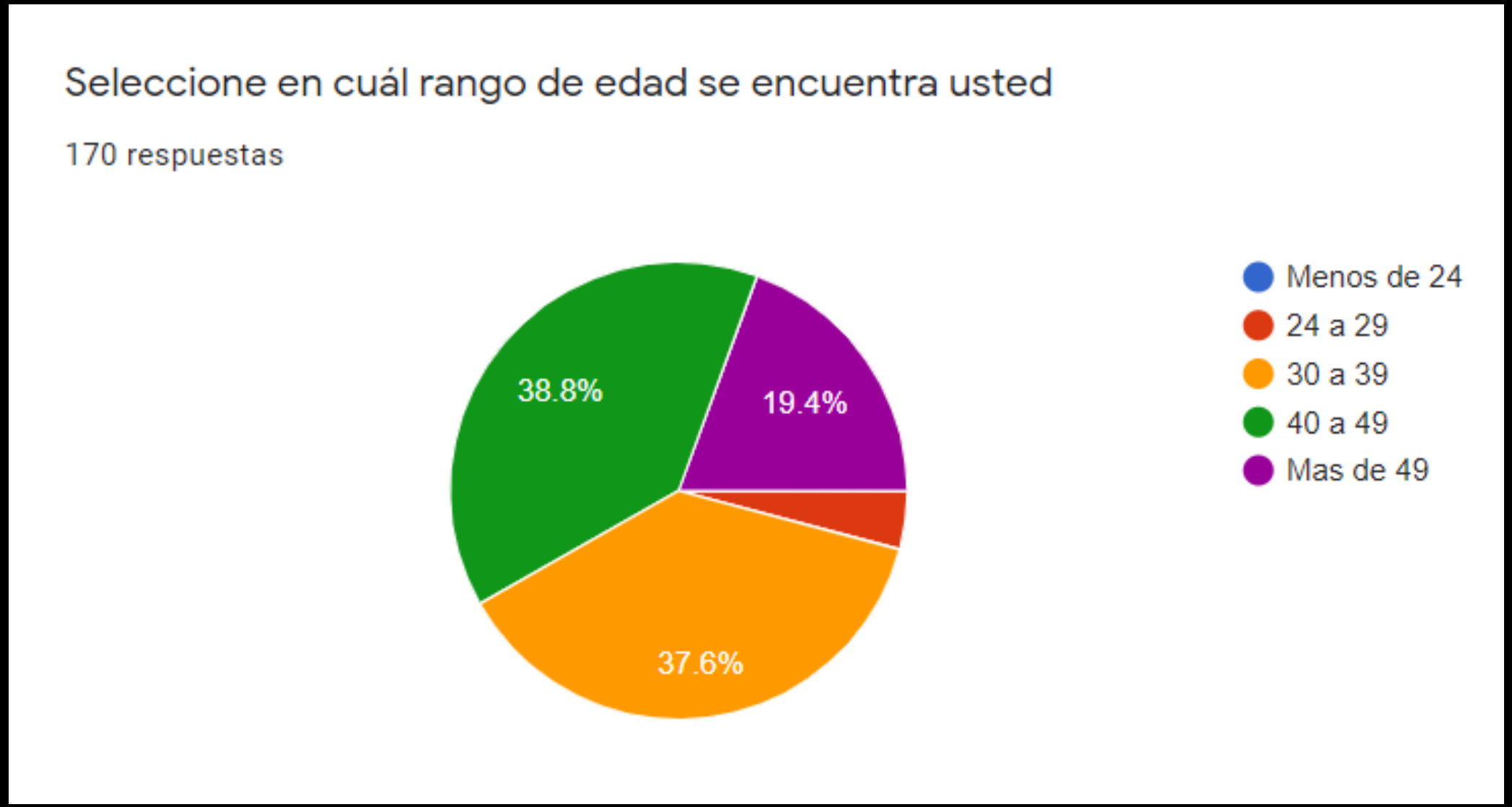
METODOLOGÍA Y MUESTRA
Fase 2 cuantitativa

El cuestionario consta de 3 secciones:

- Inventario de recursos y actividades de las áreas de ciberseguridad
- Importancia de la comunicación y participación
- Principales problemas que enfrentan

PRINCIPALES HALLAZGOS

EDADES DE LOS ENCUESTADOS

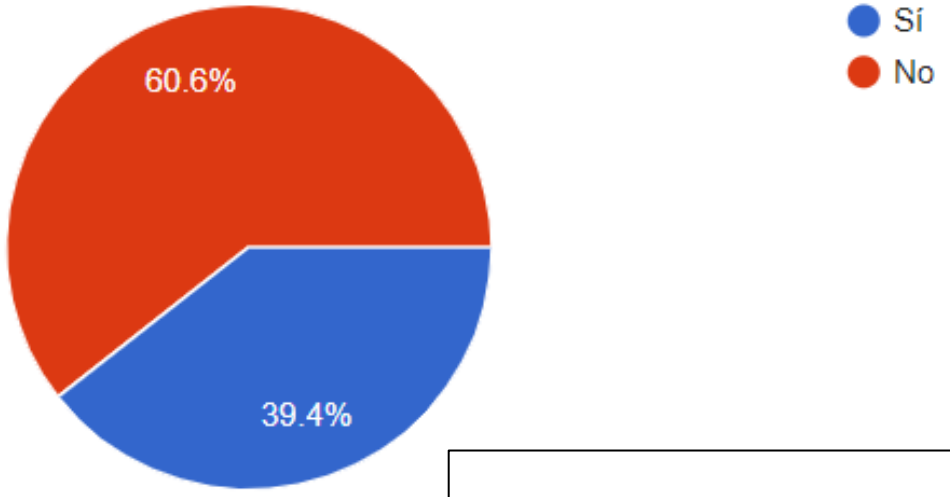


76% tienen entre 30 – 49 años.

HABLEMOS SOBRE EL ÁREA DE NOC

¿Cuenta con un área de operación y monitoreo de la red (NOC)?

170 respuestas



60.6% **no** cuenta con área NOC

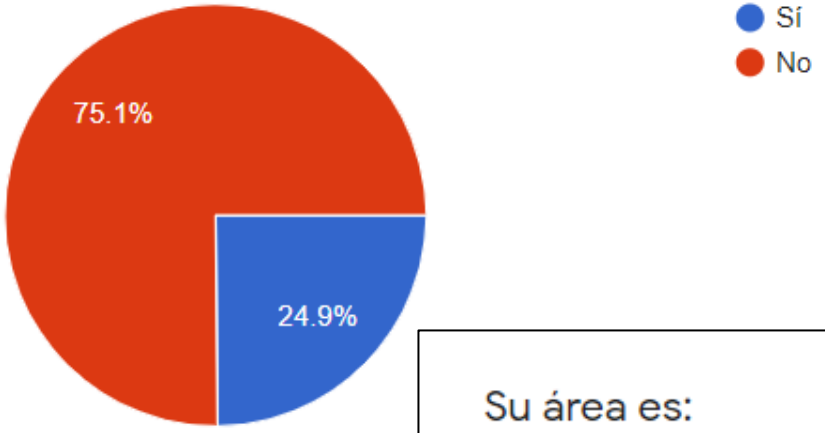
Cuando se tiene área NOC en el 55.2% de los casos funciona para todos los planteles

Esta área funciona para:

67 respuestas

¿Cuenta con área de ciberseguridad?

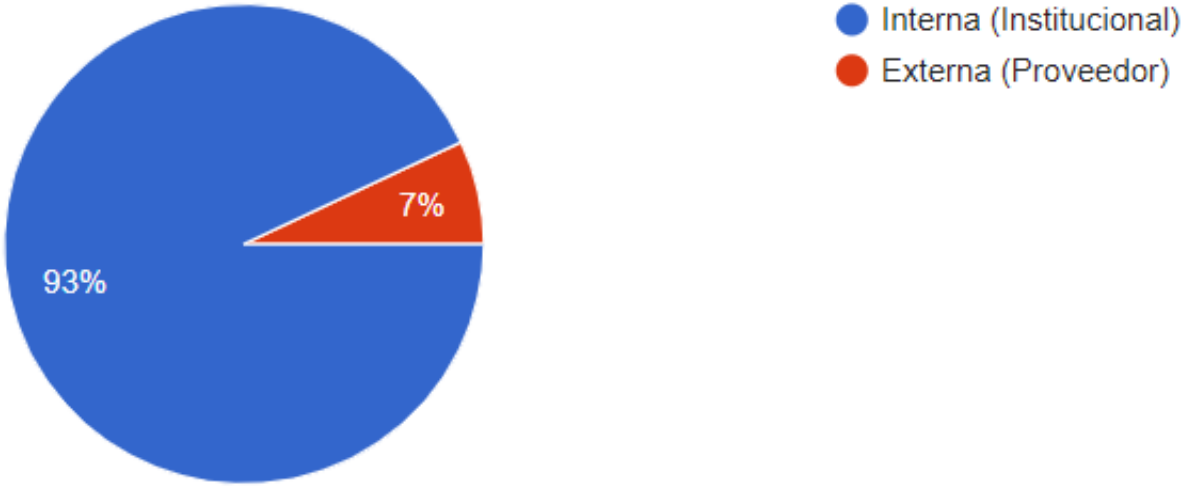
169 respuestas



75.1% **no** cuenta con área de ciberseguridad

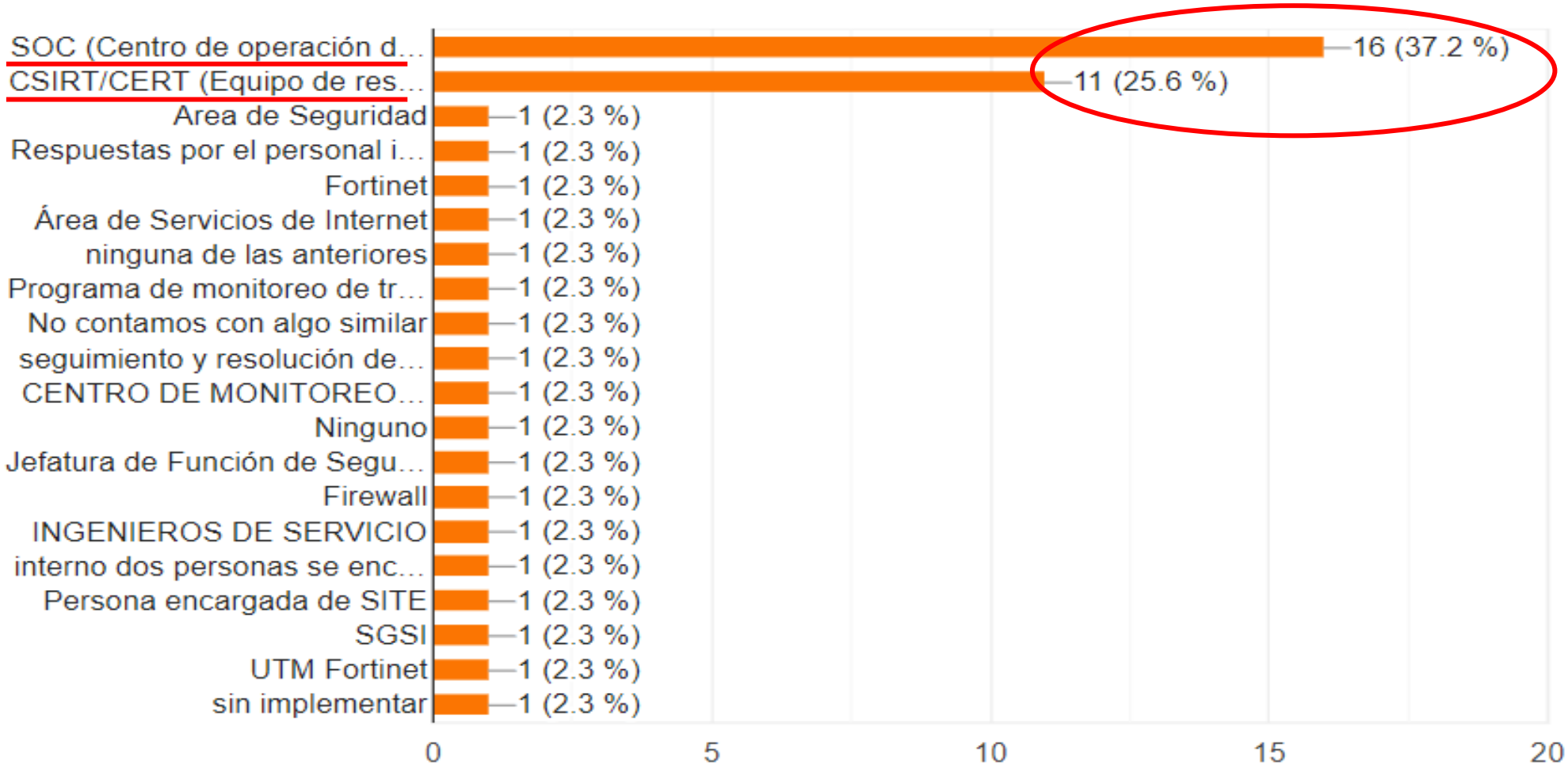
Su área es:

43 respuestas



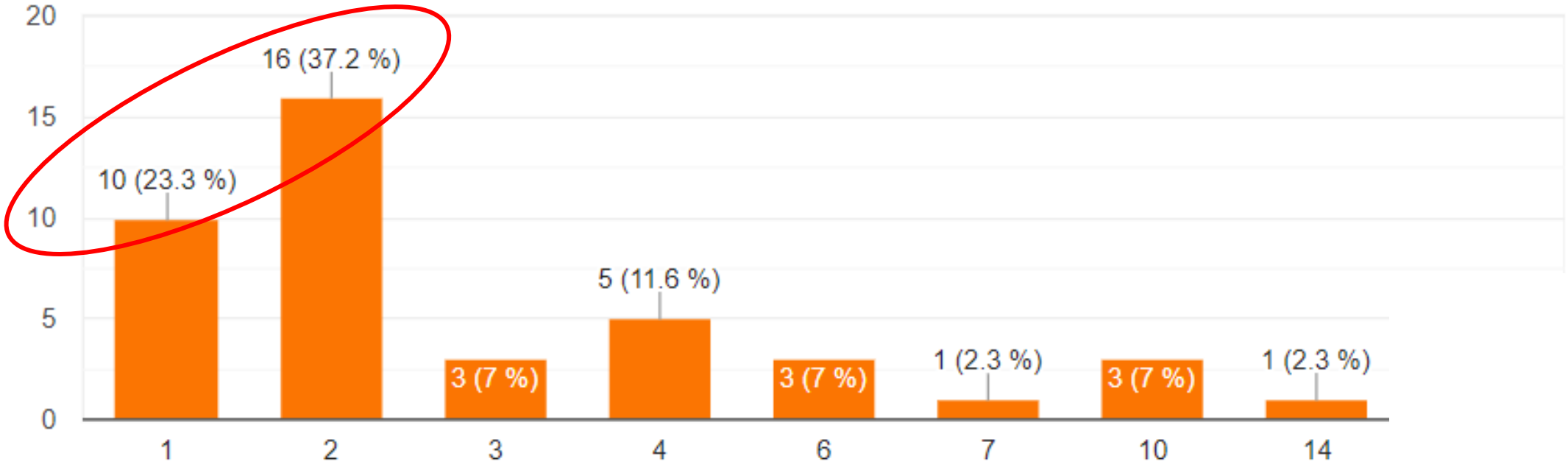
Cuenta con un:

43 respuestas



Número de personas que laboran en esta área

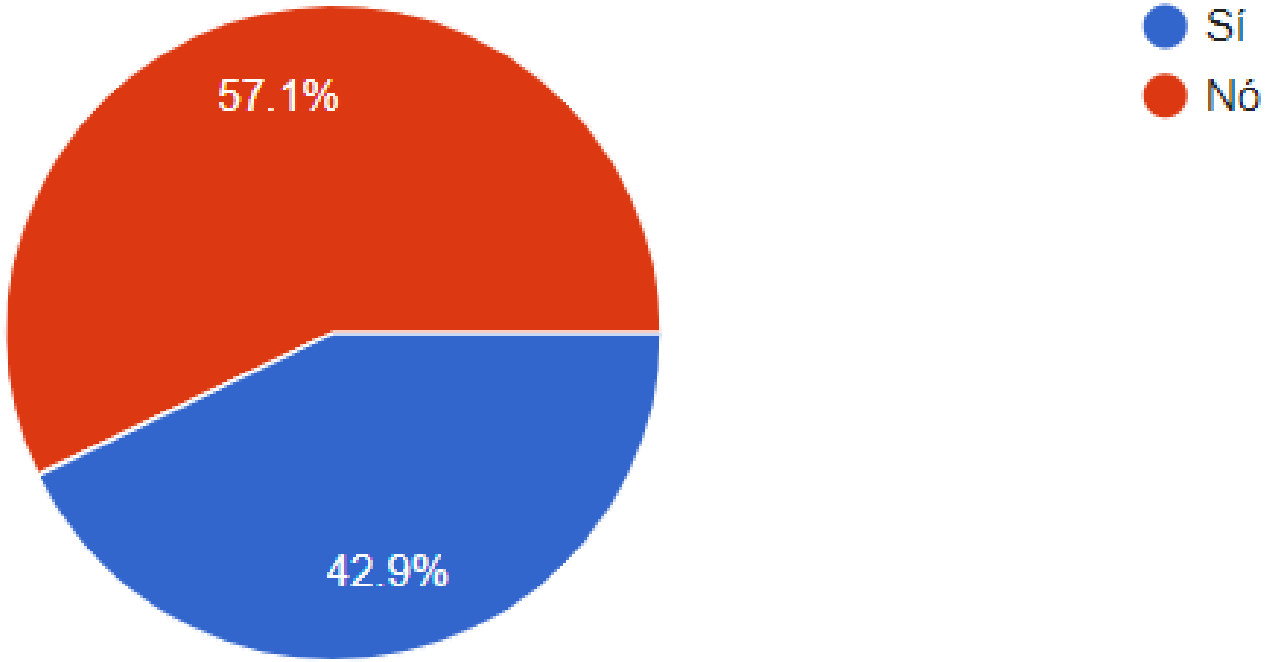
43 respuestas



60.5% cuenta con 1 a 2 personas en el área

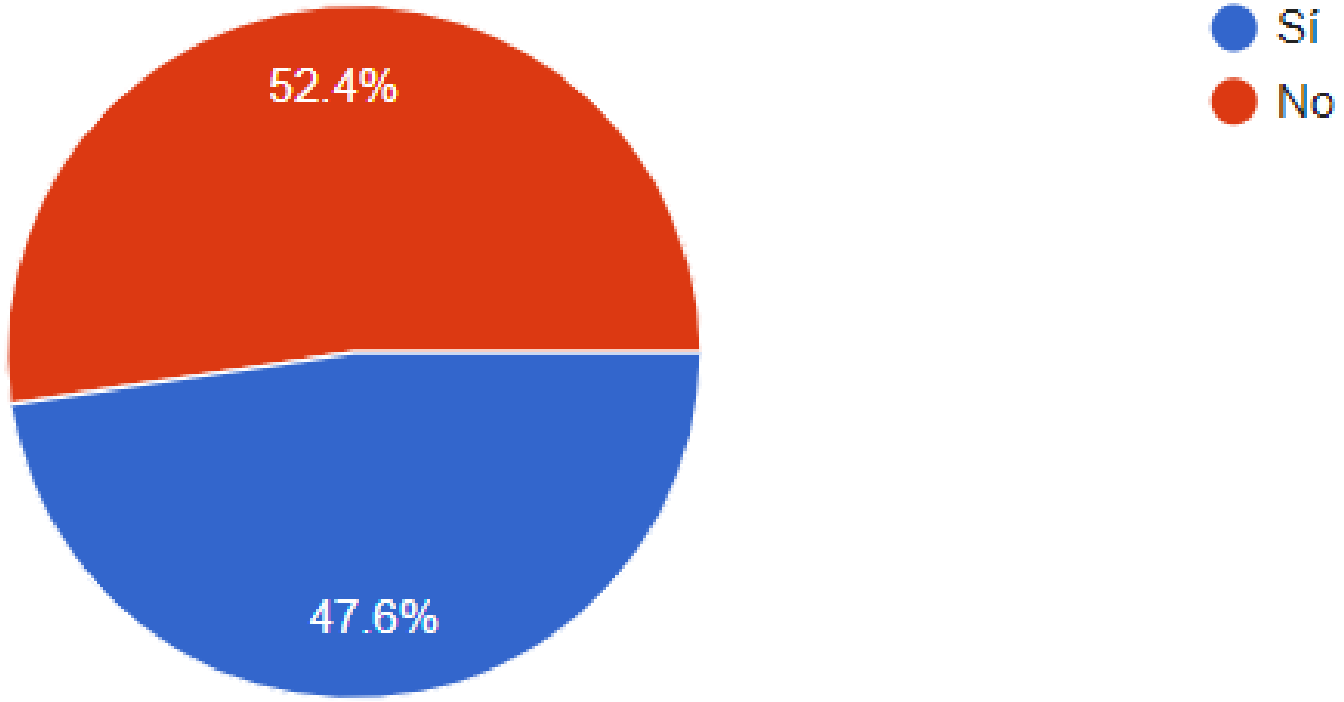
¿Cuenta con un Sistema de Gestión de la Seguridad de la Información?

42 respuestas



¿Cuenta con algún sistema para la gestión de incidentes?

42 respuestas

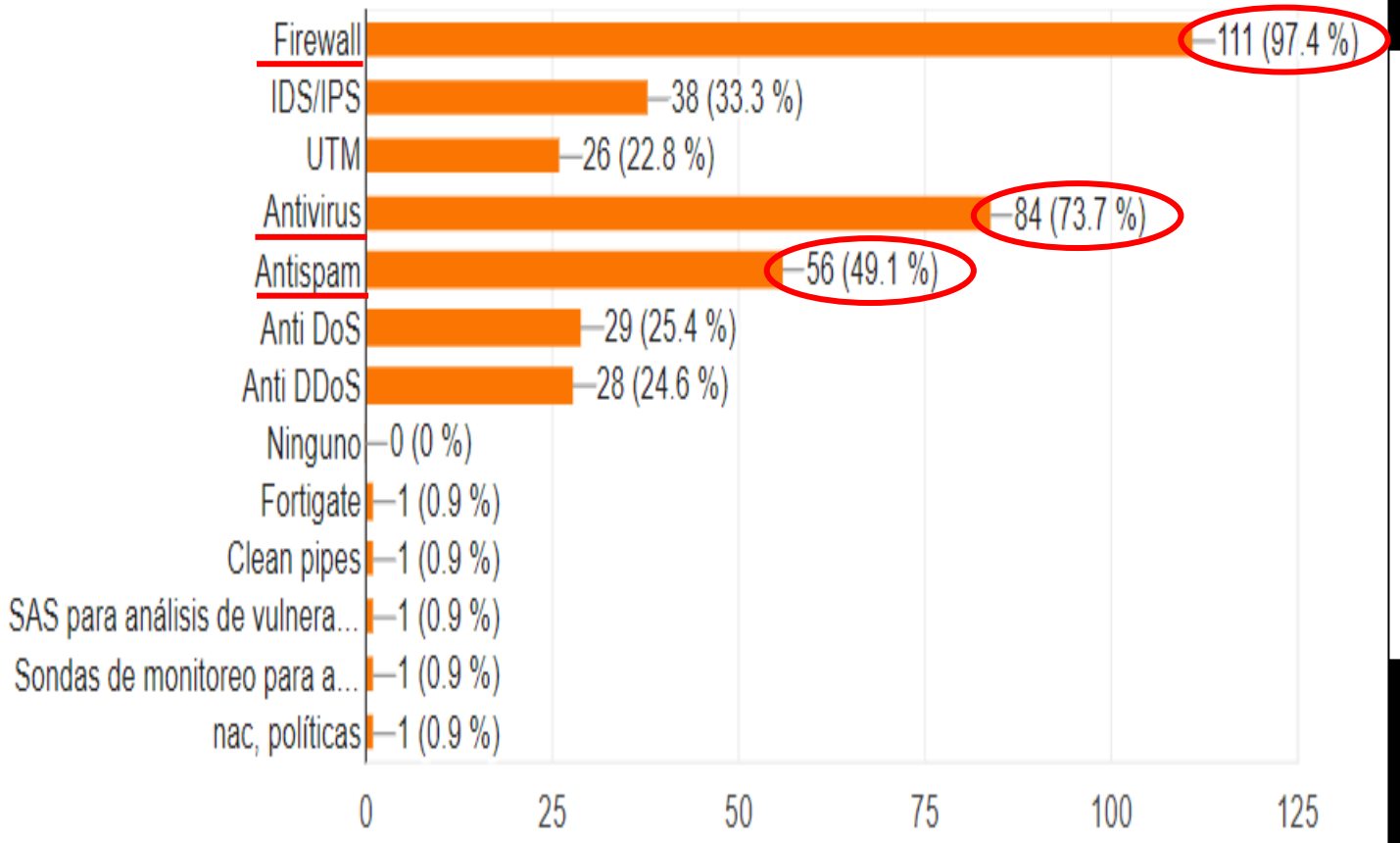


HABLEMOS SOBRE LA INFRAESTRUCTURA DE SEGURIDAD

CSIRT

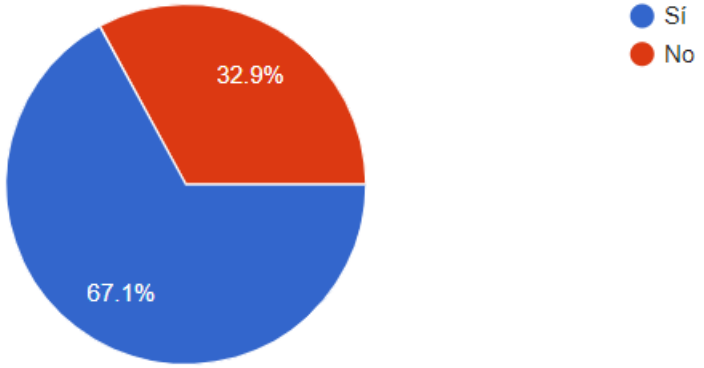
De los siguientes elementos, ¿cuáles son con los que cuentan?

114 respuestas

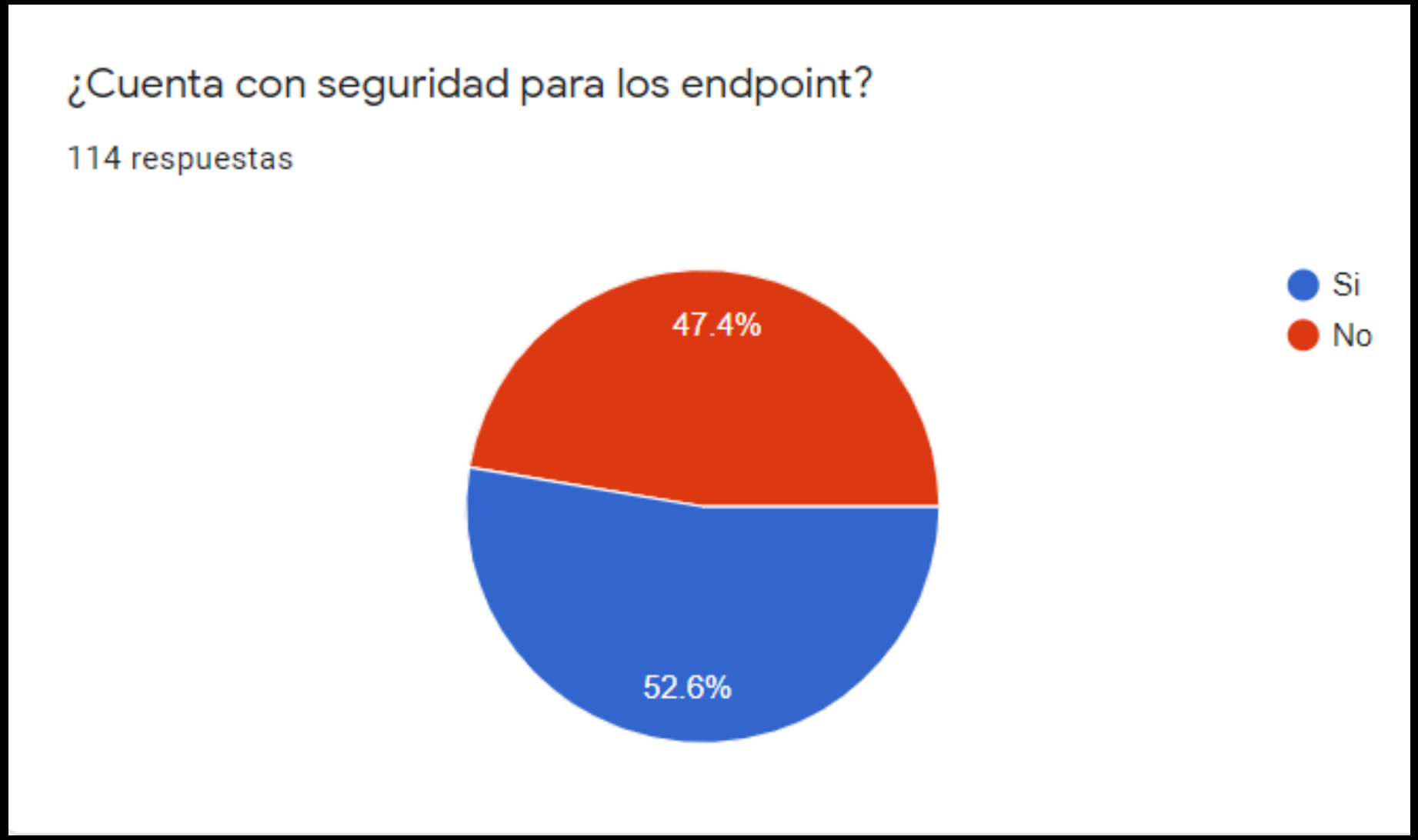


¿Cuentan con infraestructura de seguridad institucional?

170 respuestas



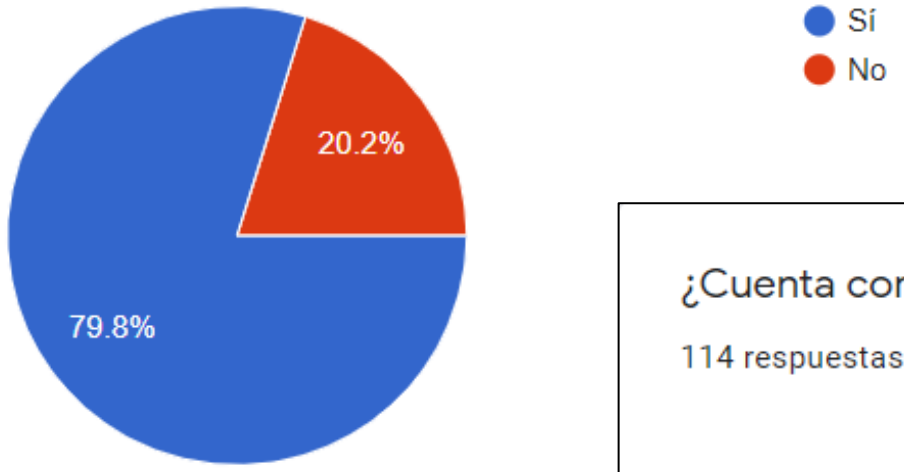
67.1% cuenta con infraestructura de seguridad institucional



52.6% cuenta con seguridad para los *endpoint*.
En 6 de cada 10 casos es *on premise*; en 4 de cada 10 es en la nube.

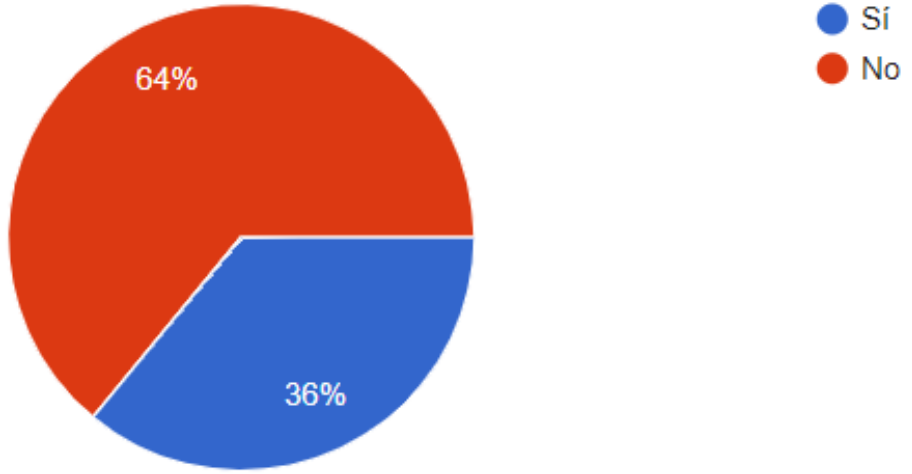
En caso de pérdida por ataque cibernético, ¿cuenta con sistema de respaldo para la recuperación de la información?

114 respuestas



¿Cuenta con un plan o proceso de recuperación de desastres?

114 respuestas



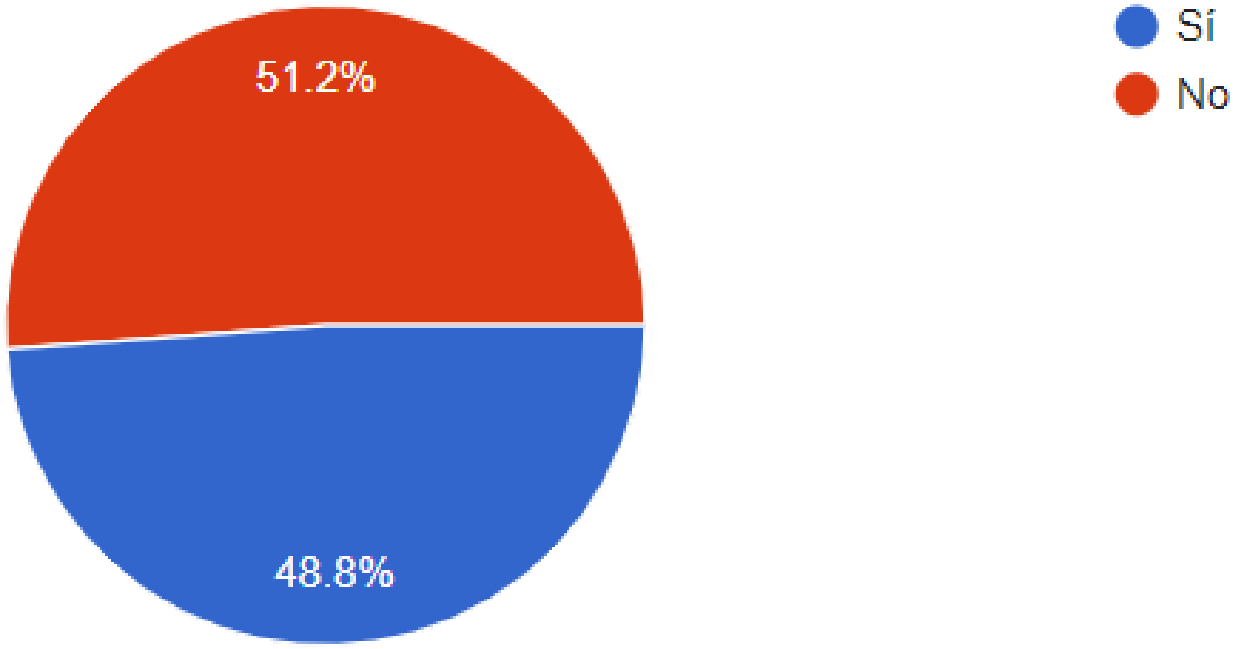
Aunque 79.8% cuenta con sistema de respaldo, el 64% no tiene un plan o proceso de recuperación de desastres

HABLEMOS SOBRE ESTÁNDARES Y POLÍTICAS DE SEGURIDAD

CSIRT

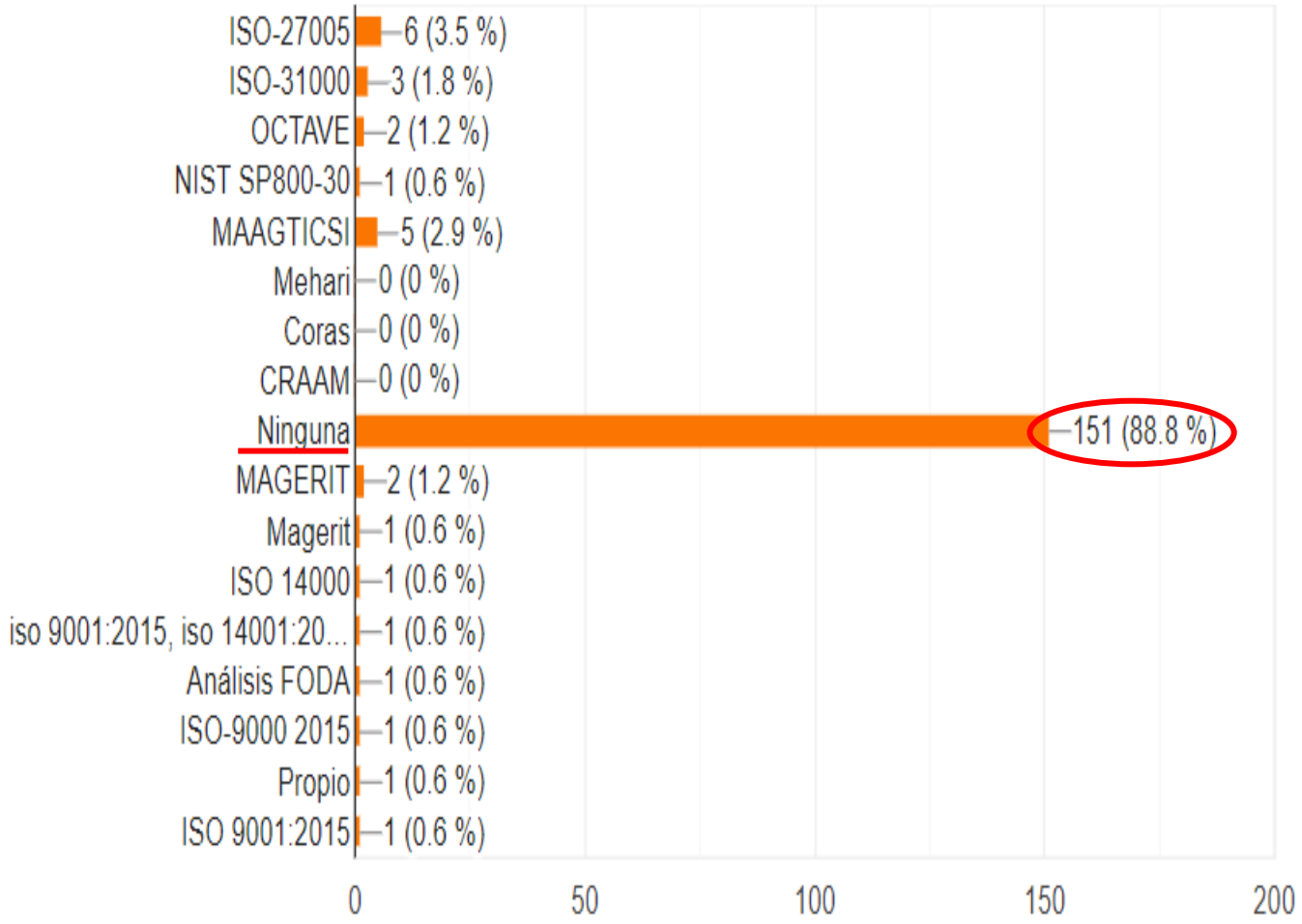
¿Cuenta con políticas de ciberseguridad?

170 respuestas



De las siguientes metodologías de análisis de riesgo ¿ha implementado alguna en su institución?

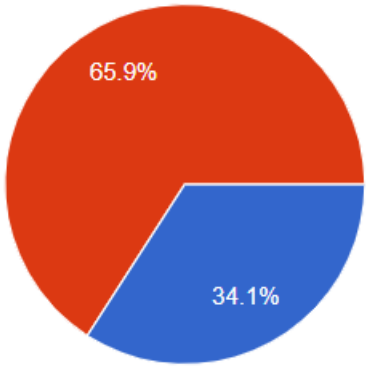
170 respuestas



¿Cuenta con un plan de gestión de riesgos?

170 respuestas

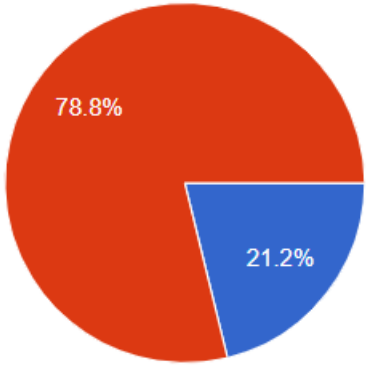
65.9% **no** cuenta con un plan de gestión de riesgos



¿Tiene implementado el proceso de gestión y manejo de riesgos?

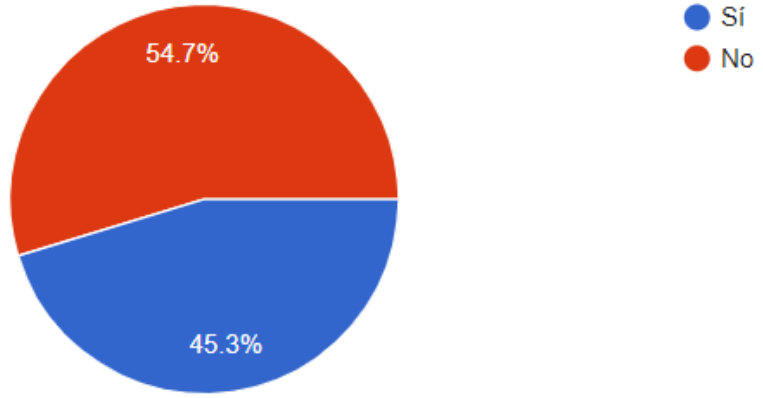
170 respuestas

78.8% **no** tiene implementado el proceso de gestión y manejo de riesgos



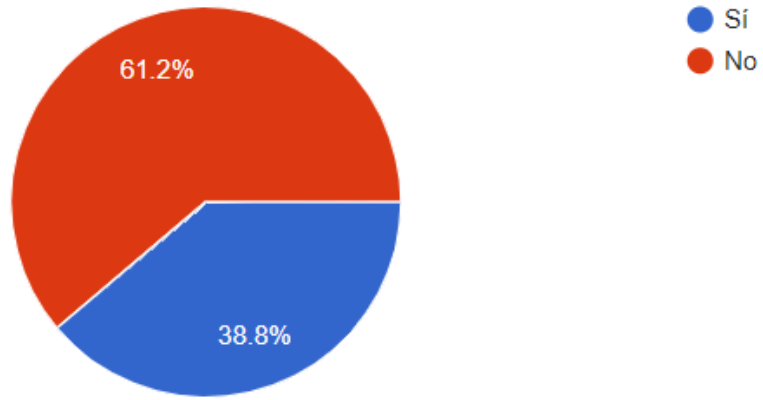
¿Realiza análisis de riesgo al menos una vez al año?

170 respuestas



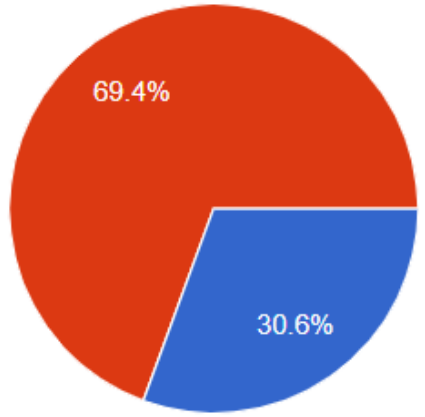
¿Realiza análisis de vulnerabilidad al menos una vez al año?

170 respuestas



¿Realiza pruebas de penetración al menos una vez al año?

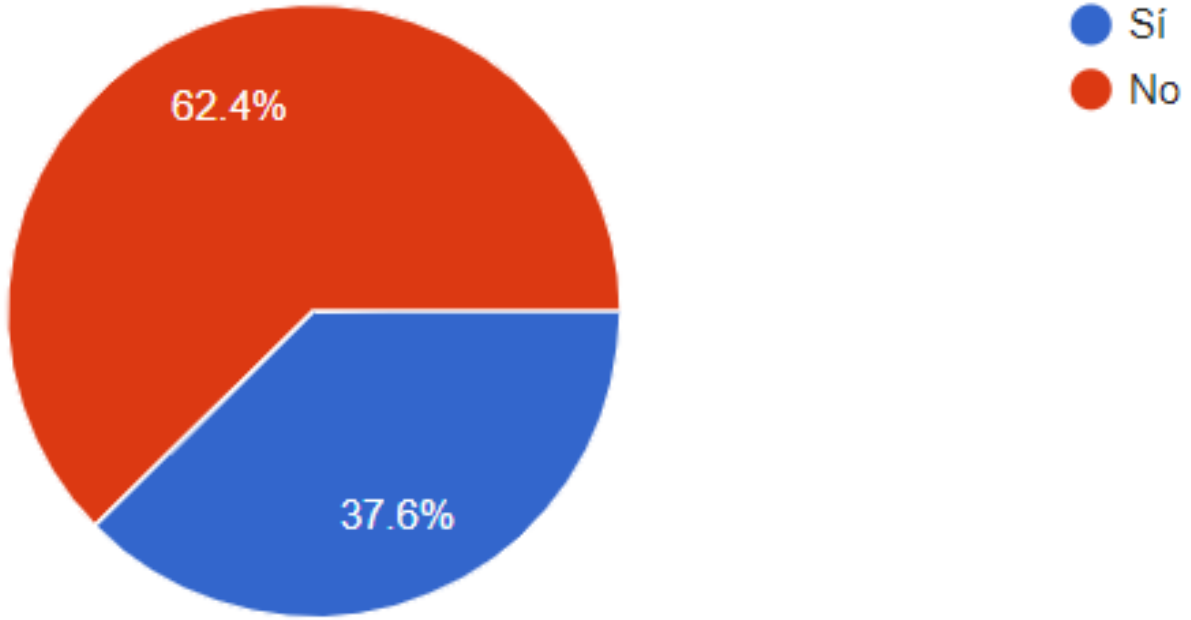
170 respuestas



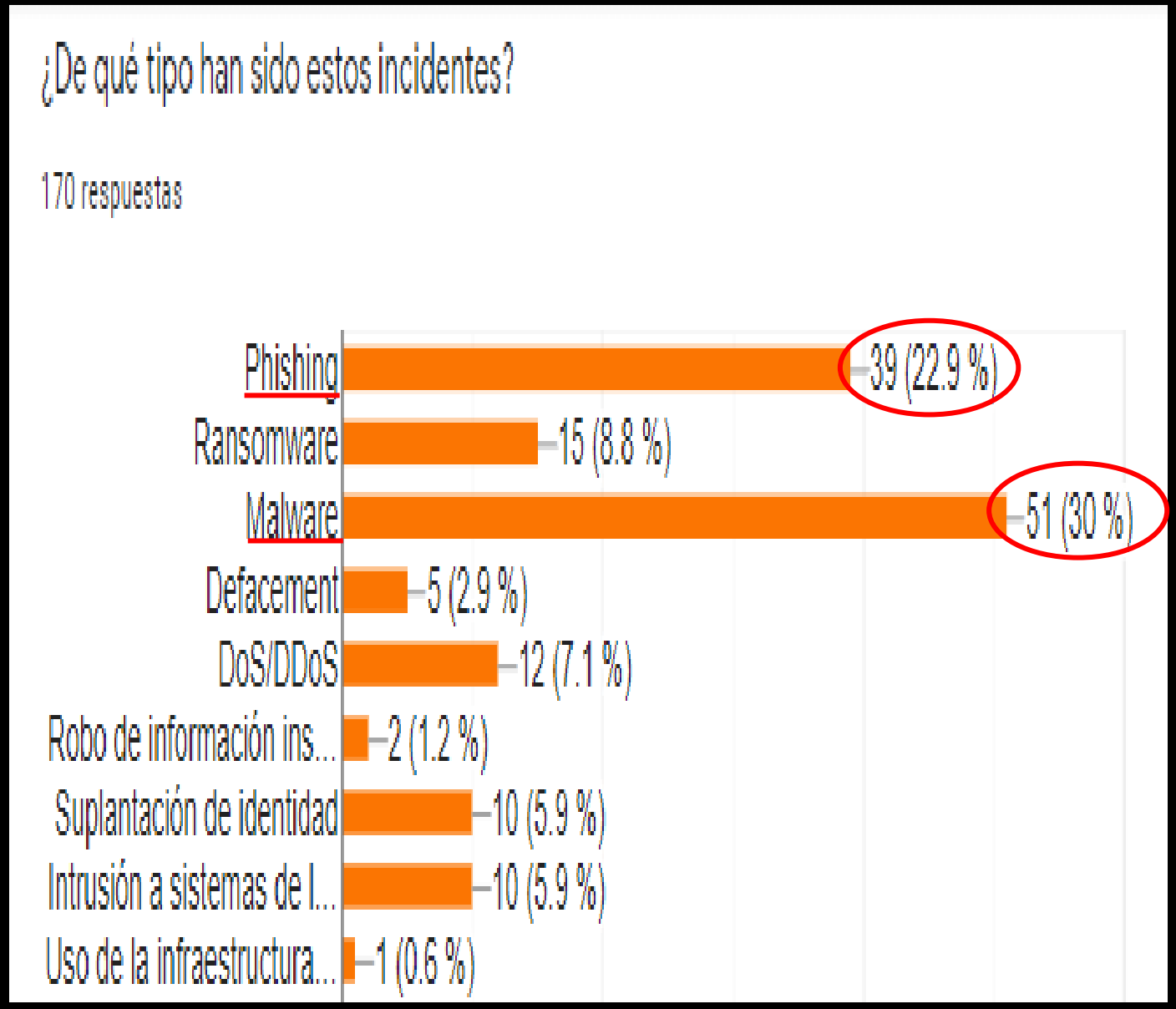
Tendencia a no realizar análisis de riesgo o de vulnerabilidad, ni pruebas de penetración anuales

¿Realiza pruebas de seguridad al código fuente a las aplicaciones de desarrollo interno?

170 respuestas



HABLEMOS SOBRE LA GESTIÓN DE LA SEGURIDAD

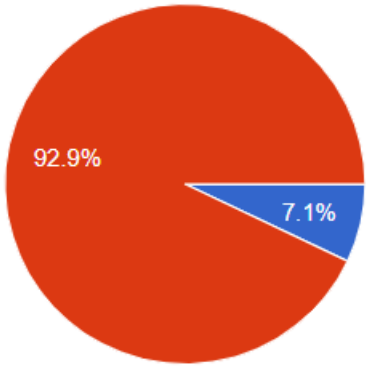


El 64.1% dice no haber sufrido o no haberse dado cuenta de ciberataques en los últimos 12 meses

"Muchas veces no sabemos realmente si hemos sufrido un ataque por no contar con los elementos para detectarlo" (comentario en grupo de enfoque)

¿Cuenta con un plan de capacitación/certificación en ciberseguridad para el personal de Dirección/Estrategia?

170 respuestas

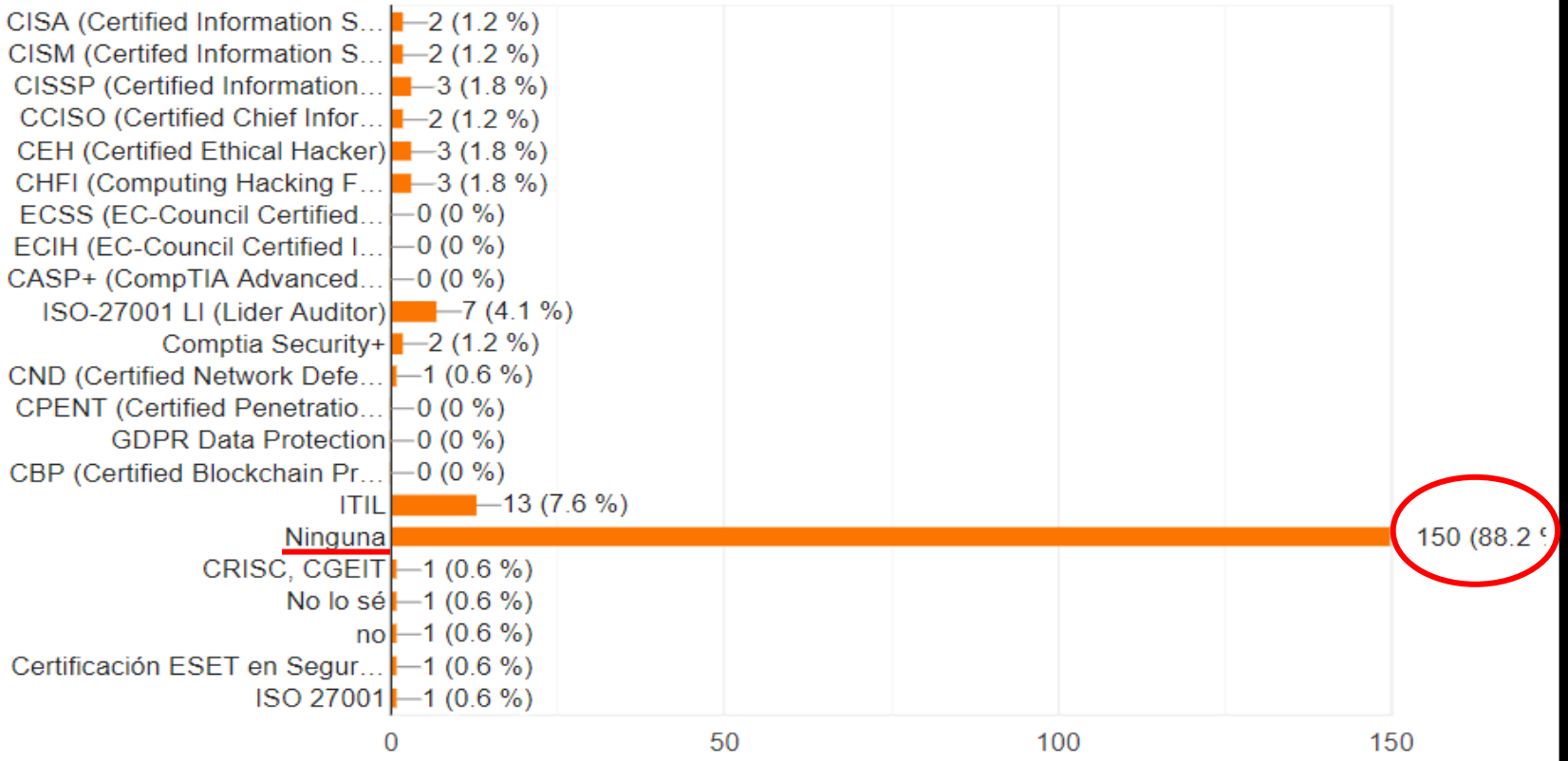


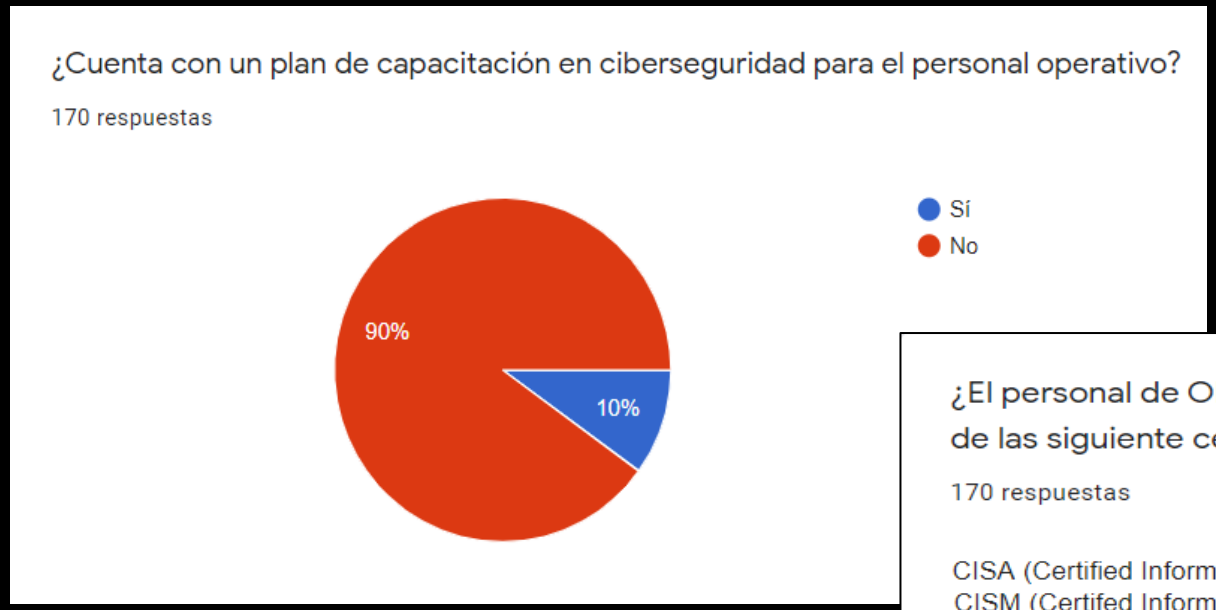
Sí
No

El 92.9% del personal de dirección/estrategia **no** cuenta con un plan de certificación

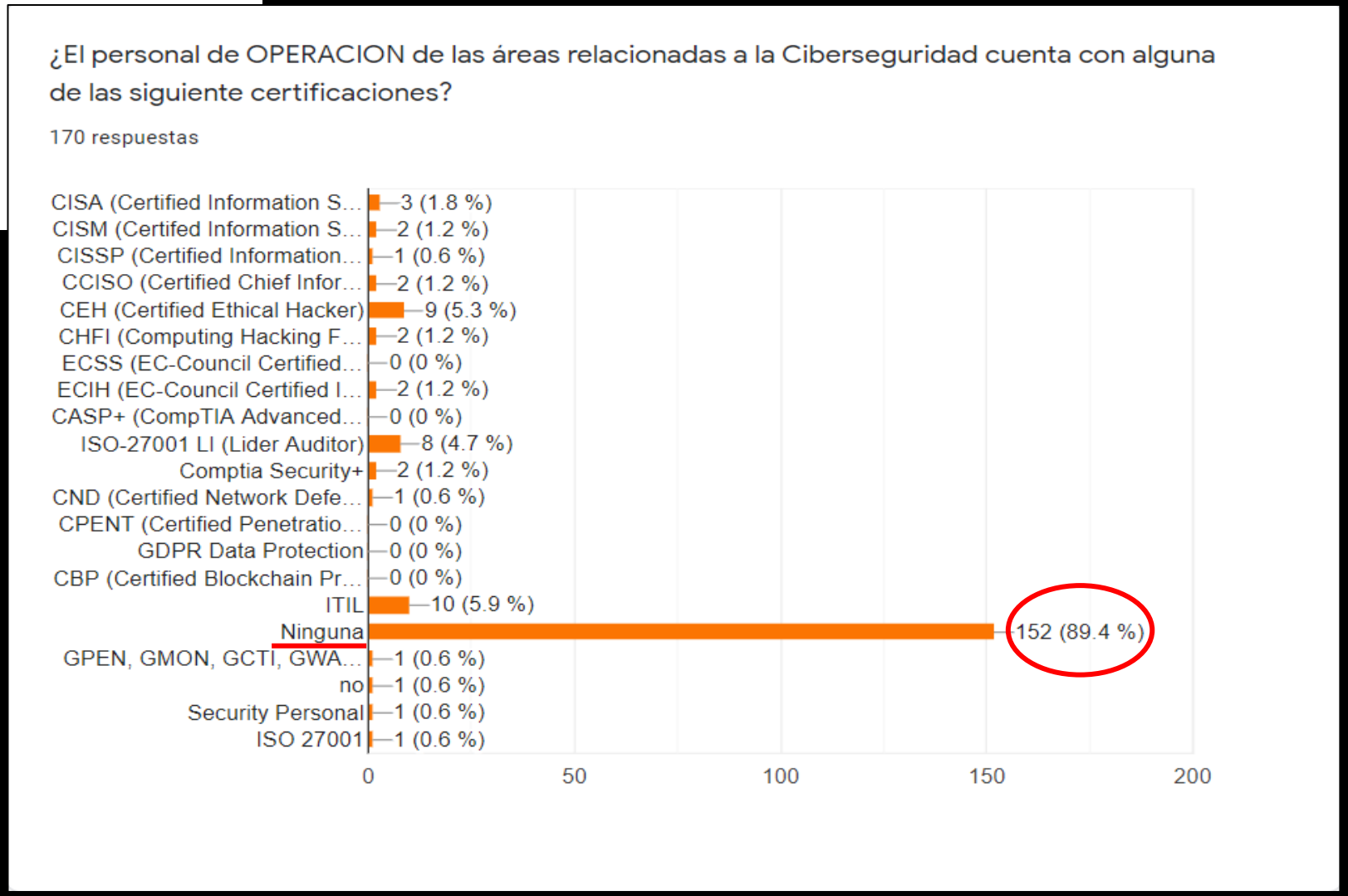
¿El personal de DIRECCIÓN / ESTRATEGIA de las áreas relacionadas a la Ciberseguridad cuenta con alguna de las siguiente certificaciones?

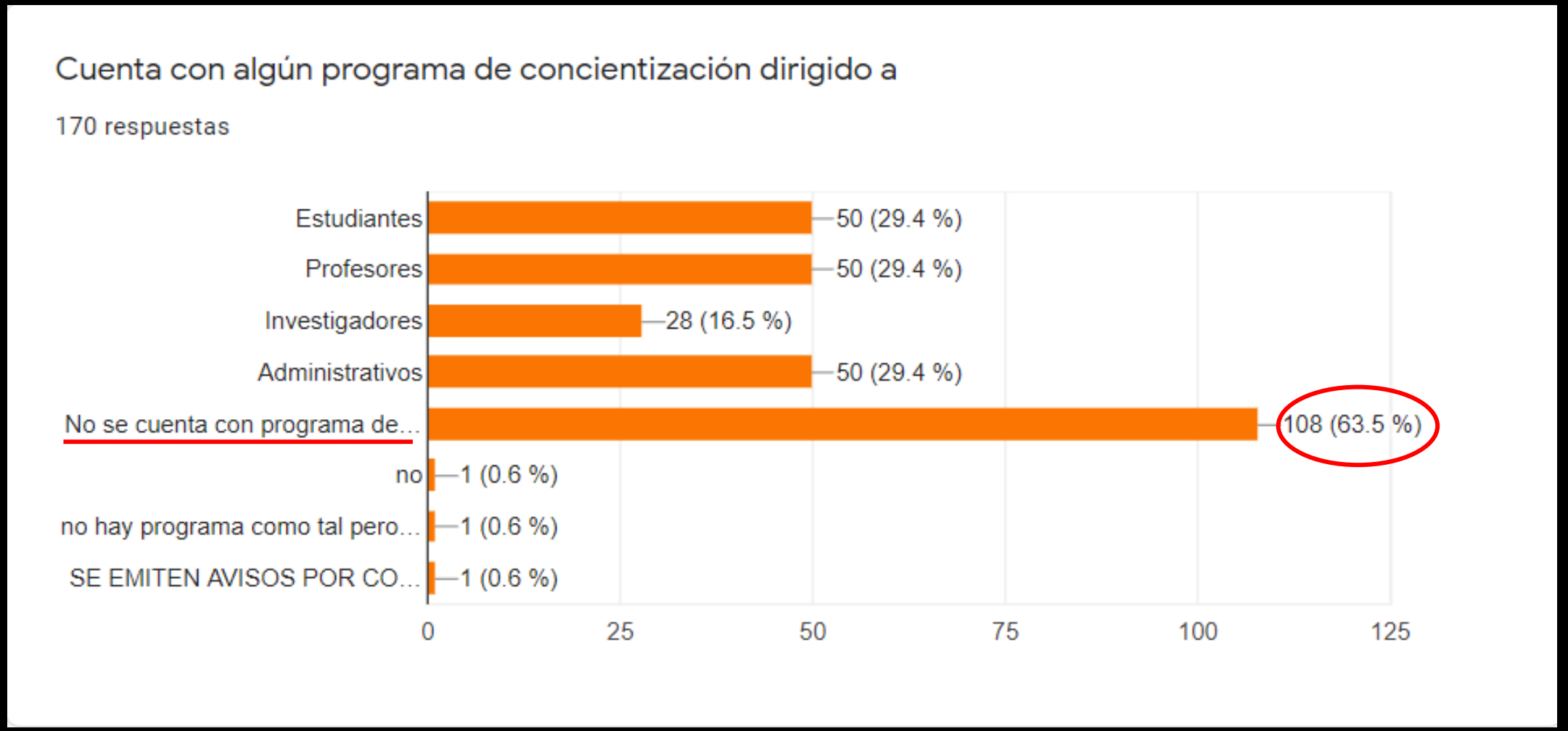
170 respuestas





El 90% del personal operativo **no** cuenta con un plan de certificación

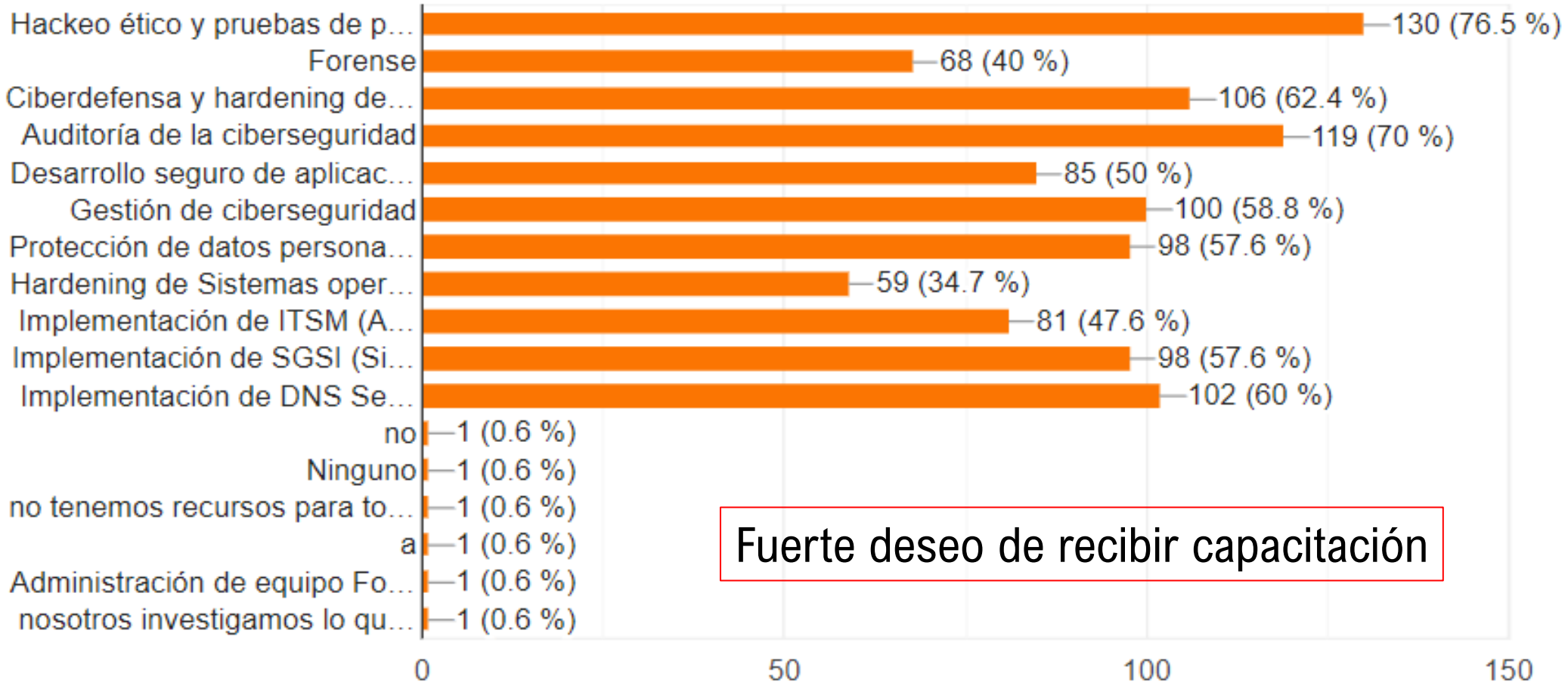




El 63.5% **no** cuenta con un programa de concientización para los usuarios finales

¿Qué tipo de capacitación le gustaría recibir para usted y el personal de las áreas de ciberseguridad?

170 respuestas



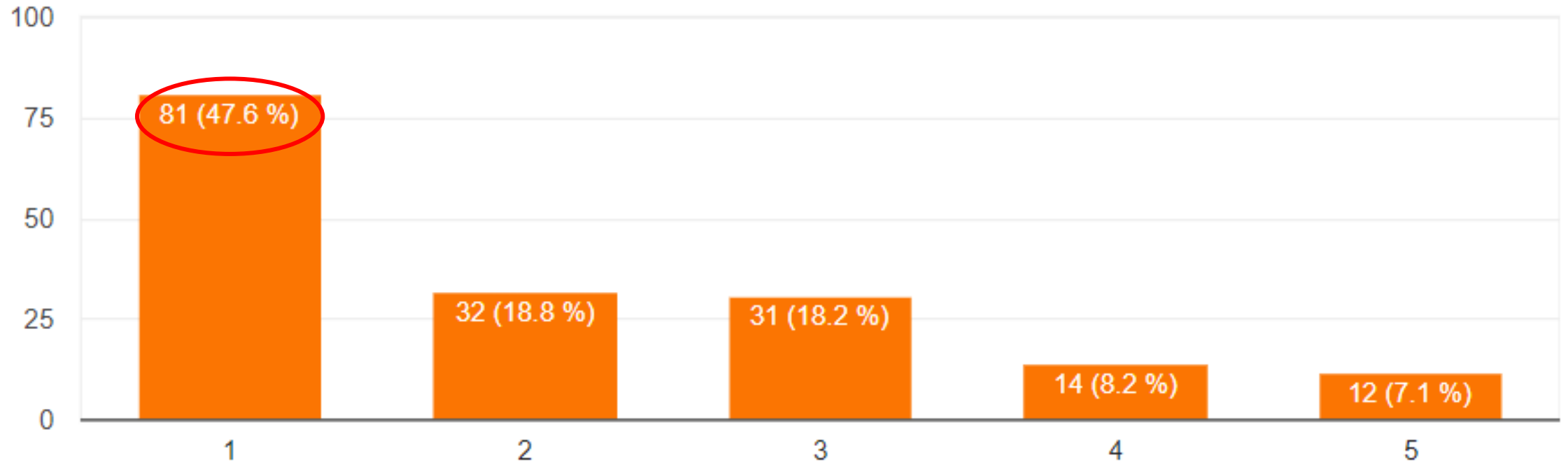
Fuerte deseo de recibir capacitación

HABLEMOS SOBRE LOS PROBLEMAS A LOS QUE SE ENFRENTAN EN SU TRABAJO DIARIO

Falta de presupuesto

170 respuestas

Promedio: 3.9; Top Box (47.6%); top 2 Box (66.4%).

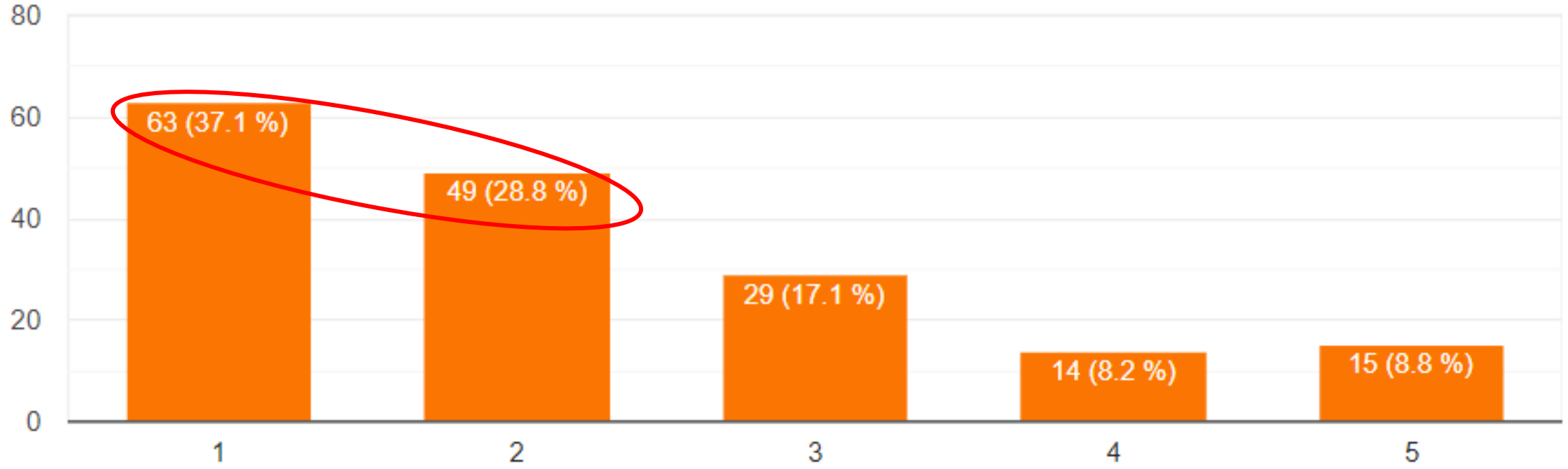


Escala de 5 puntos, donde el “1” vale 5; el “2” vale 4; el “3” vale 3; el “4” vale 2; el “5” vale 1.

Falta de recursos humanos

170 respuestas

Promedio: 3.8; Top 2 Box (65.9%).



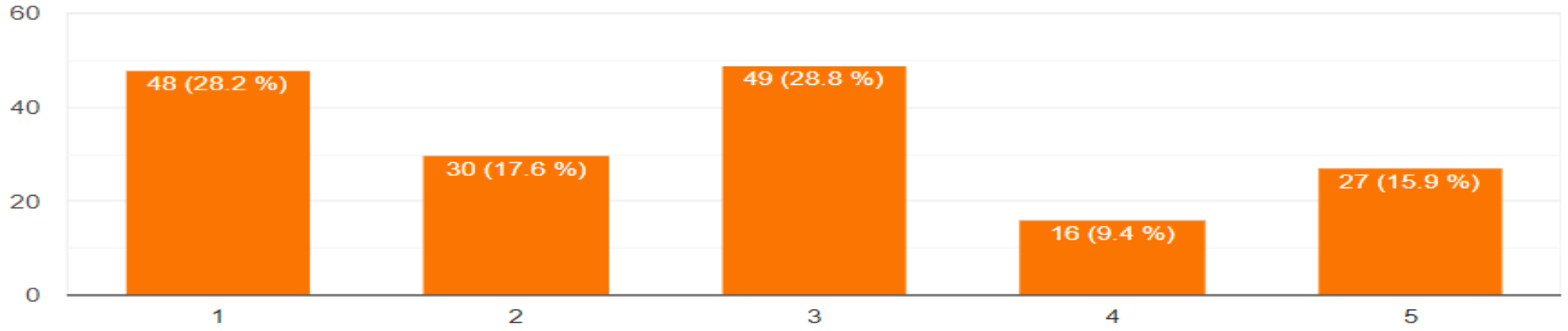
Escala de 5 puntos, donde el “1” vale 5; el “2” vale 4; el “3” vale 3; el “4” vale 2; el “5” vale 1.

PROBLEMAS POR LA FALTA DE RECURSOS HUMANOS Y SU PREPARACIÓN
Comentarios de los grupos de enfoque

- *"Hay escasez de especialistas calificados… formas especialistas y se los llevan con mejores sueldos y prestaciones, sobre todo al sector privado… y a empezar de nuevo desde cero"*
- *"Hay poco personal certificado… las certificaciones ayudan a gestionar correctamente riesgos"*
- *"Las áreas de IT se encuentran rebasadas con los cambios provocados debido al COVID"*
- *"No sabemos si estamos preparados para hacer un análisis de vulnerabilidades con el personal que tenemos"*

Ausencia de normativas

170 respuestas



Promedio: 3.3; Top 2 Box (45.8%)

Escala de 5 puntos, donde el “1” vale 5; el “2” vale 4; el “3” vale 3; el “4” vale 2; el “5” vale 1.

Las normativas no se respetan

170 respuestas

Promedio: 2.5; Bottom 2 Box (54.1%)

El problema es la ausencia de normativas, no tanto que no se respeten.

Escala de 5 puntos, donde el “1” vale 5; el “2” vale 4; el “3” vale 3; el “4” vale 2; el “5” vale 1.

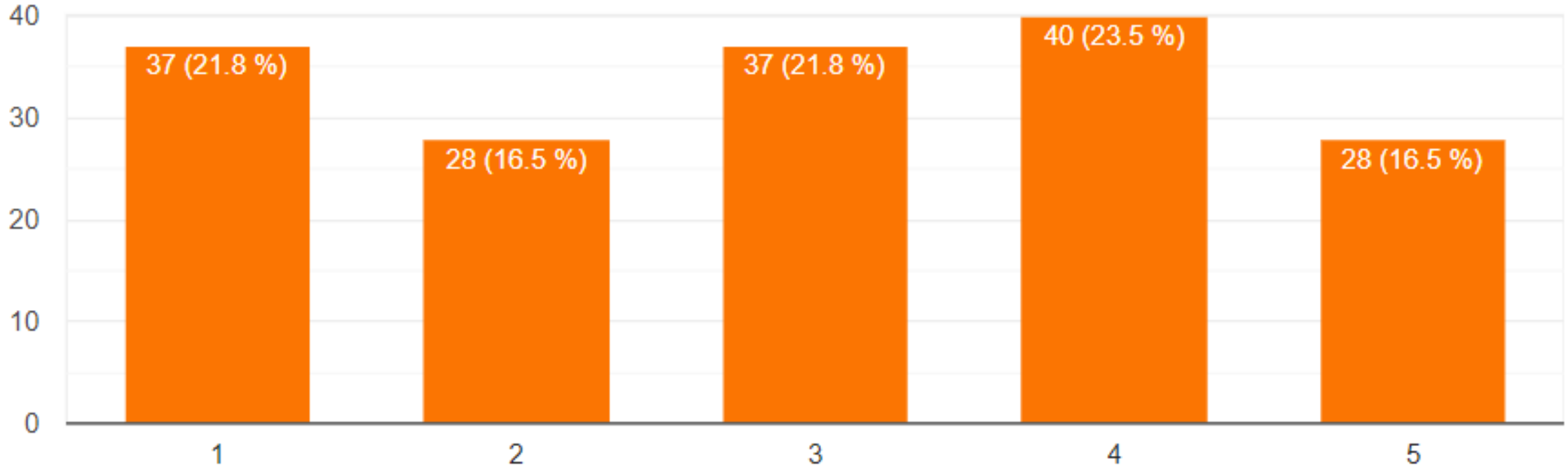
PROBLEMAS POR FALTA DE NORMATIVAS
Comentarios de los grupos de enfoque

- *"Es fundamental establecer normas y políticas de ciberseguridad para **todos** los integrantes de las instituciones y aplicarlas rigurosamente"*

Falta de conciencia del usuario final

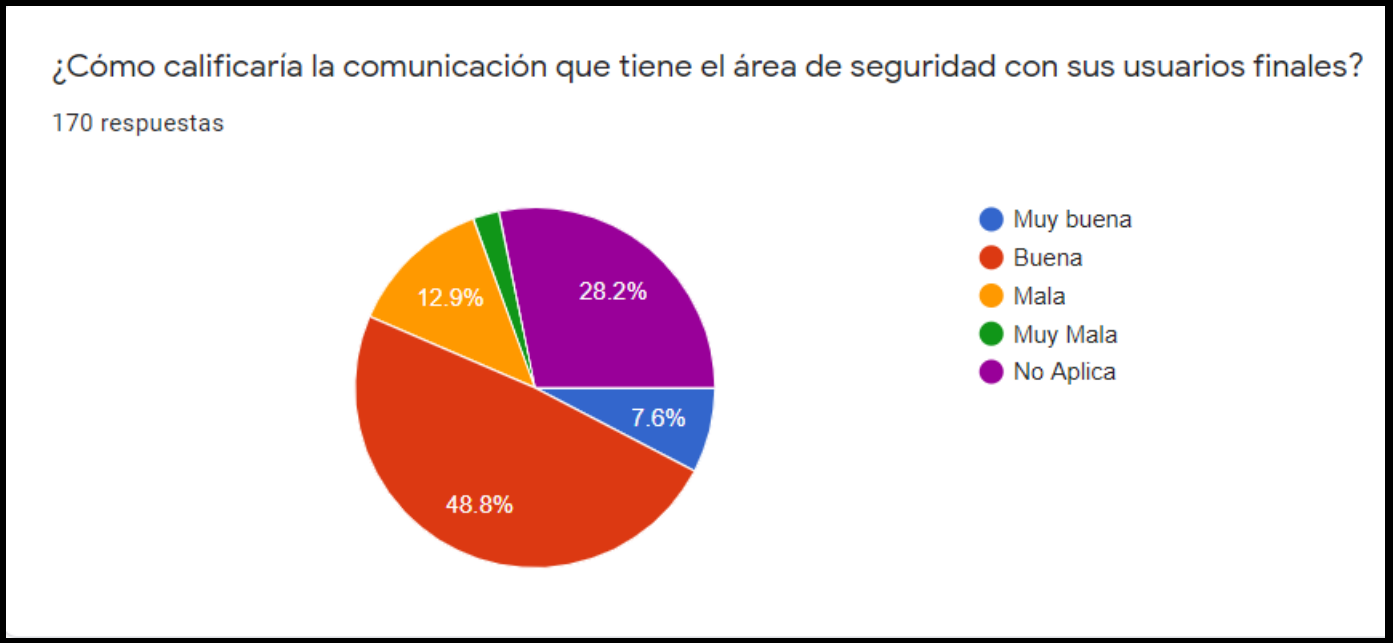
170 respuestas

Promedio: 3.0; Top 2 Box (38.3%);
Bottom 2 Box (40.0%)



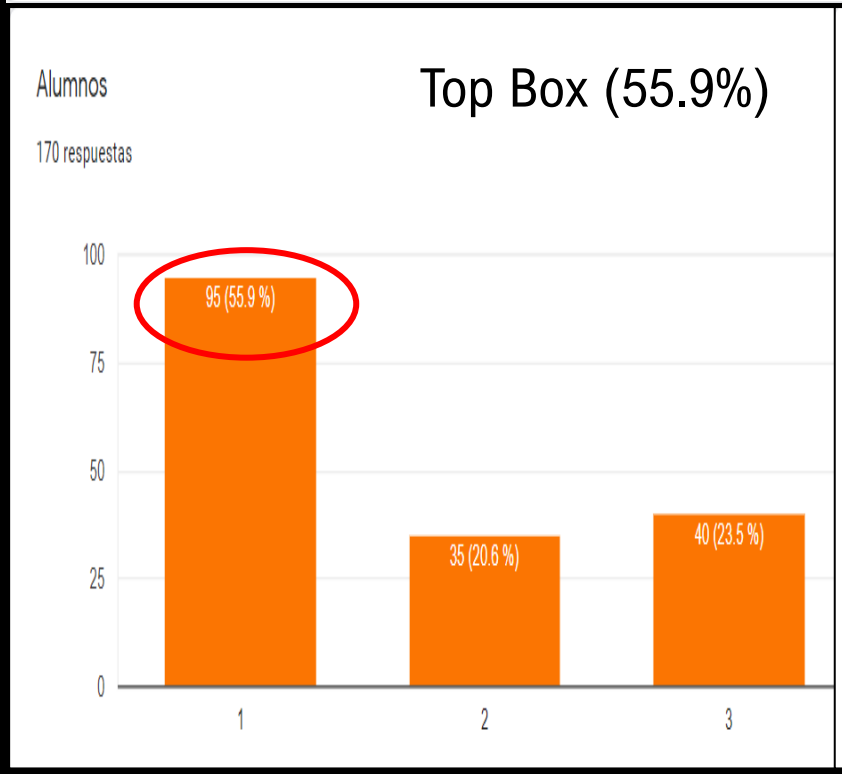
Escala de 5 puntos, donde el “1” vale 5; el “2” vale 4; el “3” vale 3; el “4” vale 2; el “5” vale 1.

Se dividen las opiniones casi por igual entre quienes tienden a considerarlo importante y quienes no.

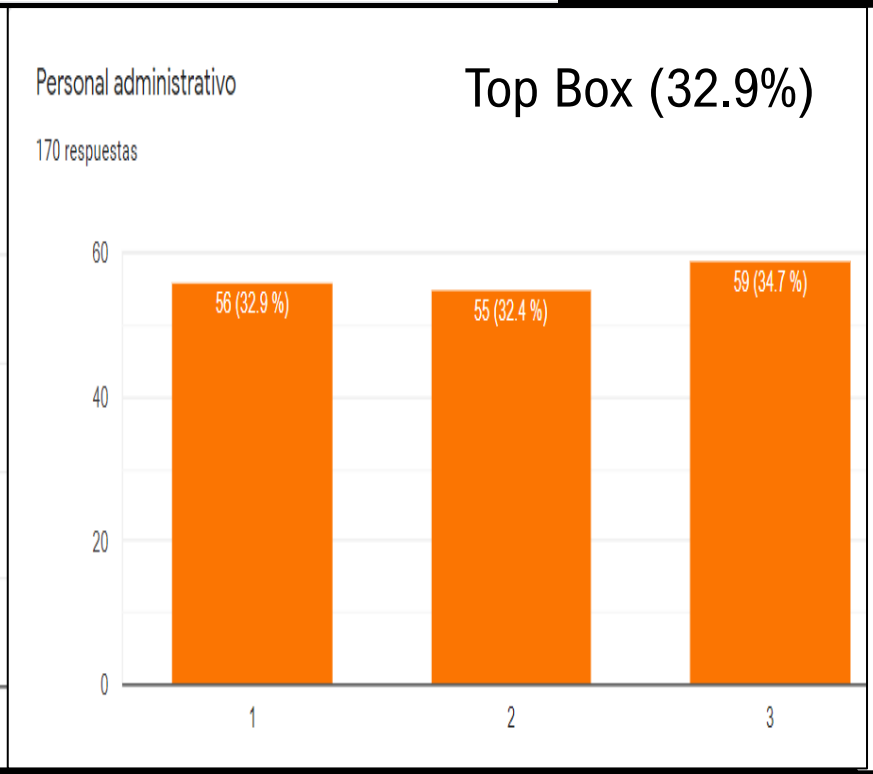


Tendencia a calificar la comunicación como buena entre quienes tienen comunicación con sus usuarios finales

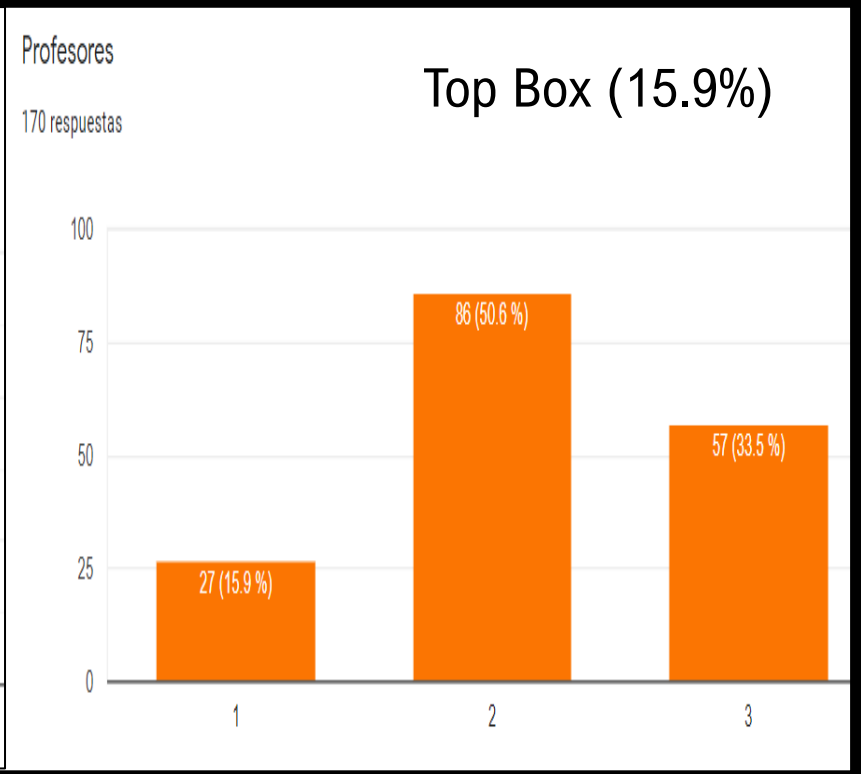
Escala de 3 puntos, donde el “1” vale 3; el “2” vale 2; el “3” vale 1



Top Box (55.9%)



Top Box (32.9%)



Top Box (15.9%)

PROBLEMAS CON EL USUARIO FINAL
Comentarios de los grupos de enfoque

- *"Falta de conocimientos e interés sobre manejo de seguridad… no se cuidan y son fácilmente engañados… son presa fácil de extorsionar"*
- *"Usan internet para fines personales como entretenimiento y comunicaciones personales"*
- *"Perciben a las normativas y a las áreas de ciberseguridad como entes que obstaculizan y solo buscan fallas"*
- *"Con el teletrabajo se incrementan los riesgos exponencialmente"*

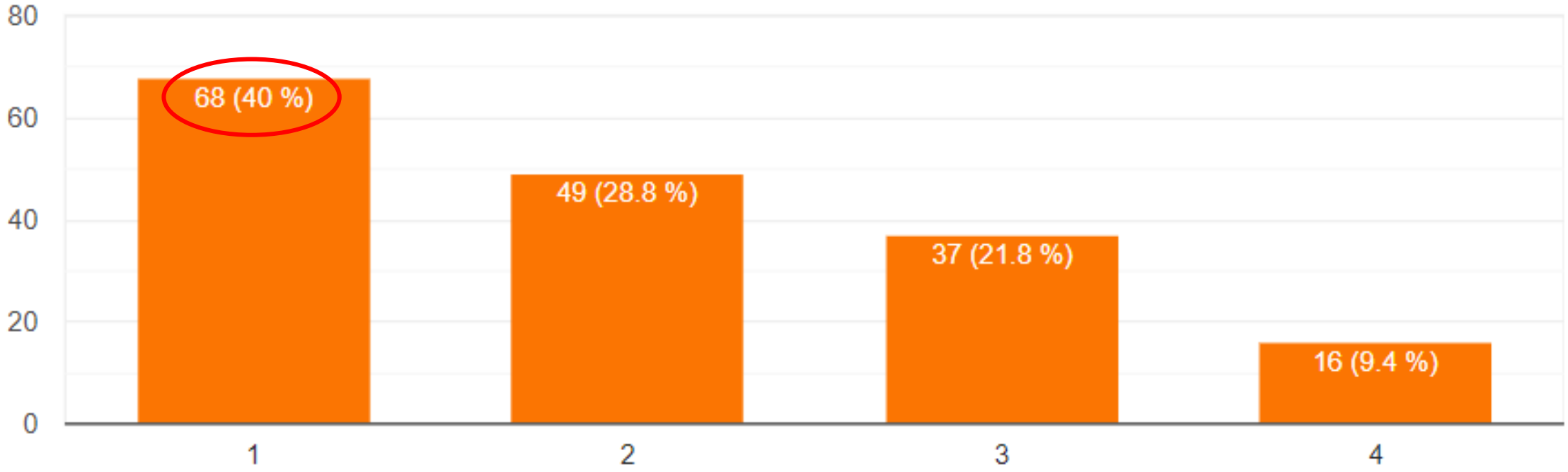
PROBLEMAS DE *COMUNICACIÓN* CON EL USUARIO FINAL
Comentarios de los grupos de enfoque

- *"Se nos percibe como el gran inquisidor que solo busca culpables en lugar de dar apoyo"*
- *"Nos cuesta comunicarnos con los usuarios y las autoridades… somos muy cerrados y técnicos"*
- *"Hay problemas de comunicación y coordinación entre las áreas de IT"*

Se ve la inversión en ciberseguridad como un gasto, no como una inversión

170 respuestas

Top 2 Box (68.8%)

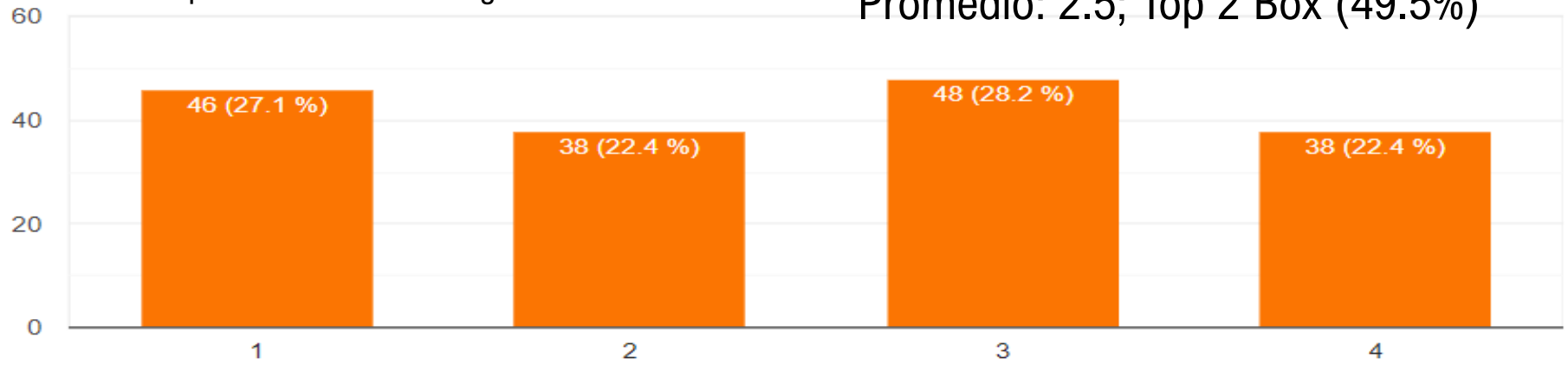


Escala de 4 puntos, donde el “1” vale 4; el “2” vale 3; el “3” vale 2; el “4” vale1.

170 respuestas

No se entiende la importancia de la ciberseguridad

Promedio: 2.5; Top 2 Box (49.5%)

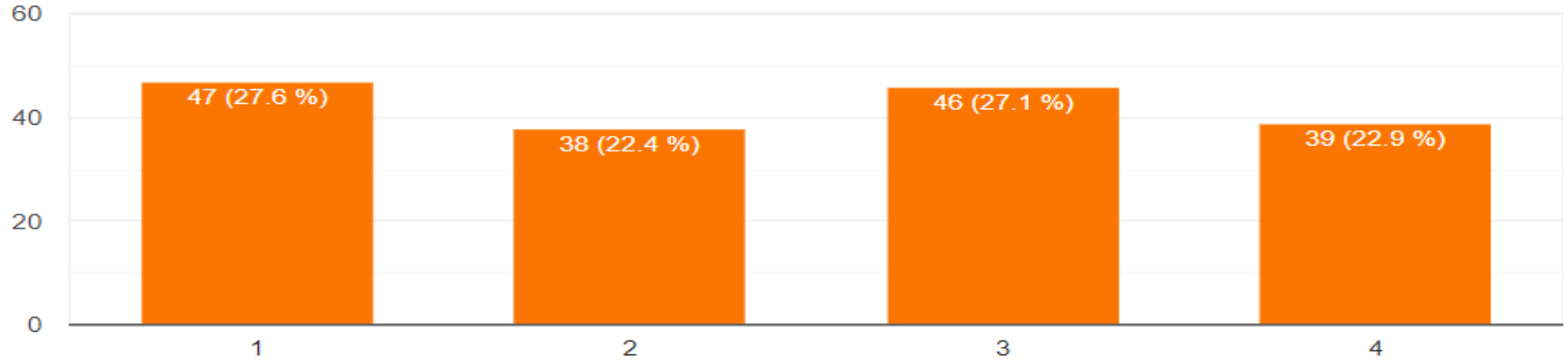


Escala de 4 puntos, donde el “1” vale 4; el “2” vale 3; el “3” vale 2; el “4” vale1

Cuando cambian las autoridades de la institución cambian las prioridades

170 respuestas

Promedio: 2.5; Top 2 Box (50.0%)



Escala de 4 puntos, donde el “1” vale 4; el “2” vale 3; el “3” vale 2; el “4” vale1

PROBLEMAS PRESUPUESTALES
Comentarios de los grupos de enfoque

- *"Muchas veces se ve a la ciberseguridad como un gasto"*
- *"Si no se han presentado problemas de ciberseguridad te dicen que no tiene justificación la inversión"*

EN CONCLUSIÓN, SUS PRINCIPALES PROBLEMAS SON…

Escala de 5 opciones	TOP BOX (%)	TOP 2 BOX (%)	PROMEDIO
Falta de presupuesto	47.6	66.4	3.9
Falta de recursos humanos	37.1	65.9	3.8
Ausencia de normativas	28.2	45.8	3.3
Falta de conciencia del usuario final	21.8	38.3	3.0
Normativas no se respetan	13.5	45.8	2.5

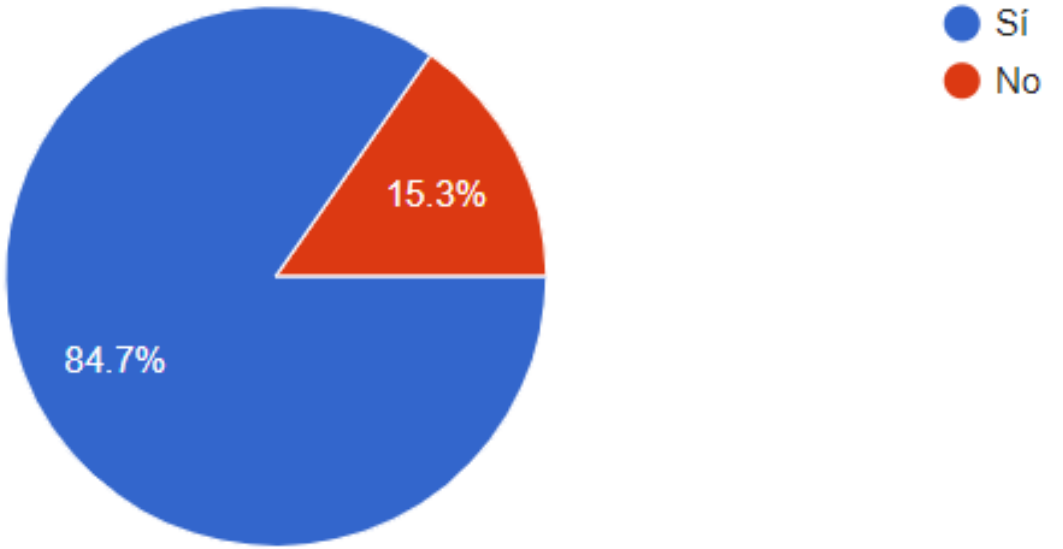
Escala de 4 opciones	TOP BOX (%)	TOP 2 BOX (%)	PROMEDIO
Recursos humanos insuficientes	62.4	80.6	3.3
Inversión en ciberseguridad se ve como gasto	40.0	68.8	3.0
Recursos humanos no certificados	32.9	55.8	2.5
Cambios de autoridades cambian las prioridades	27.6	50.0	2.5
No se entiende la importancia de la ciberseguridad	27.1	49.5	2.5

Los principales problemas: falta de presupuesto, falta de recursos humanos y la ausencia de normativas

HABLEMOS SOBRE LAS NECESIDADES DE COMUNICACIÓN Y COLABORACIÓN

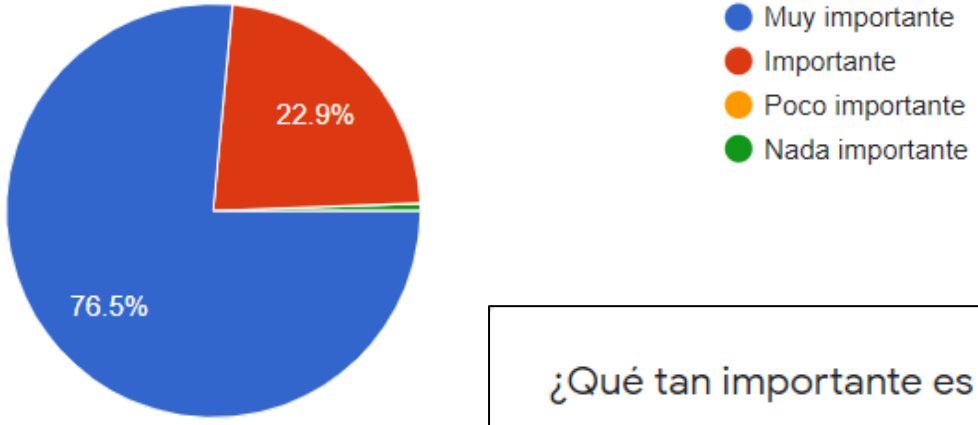
¿Estaría interesado en compartir experiencias y trabajos en grupos / encuentros / eventos de ciberseguridad organizados por las Redes Nacionales de Educación e Investigación Latinoamericanas?

170 respuestas



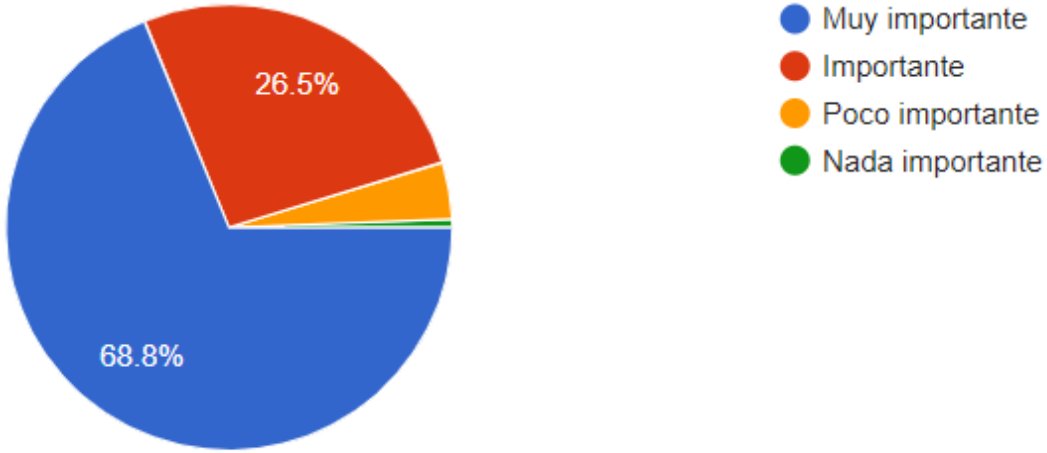
¿Qué tan importante considera que deba ser la comunicación, coordinación y apoyo entre las áreas de ciberseguridad de las IES?

170 respuestas



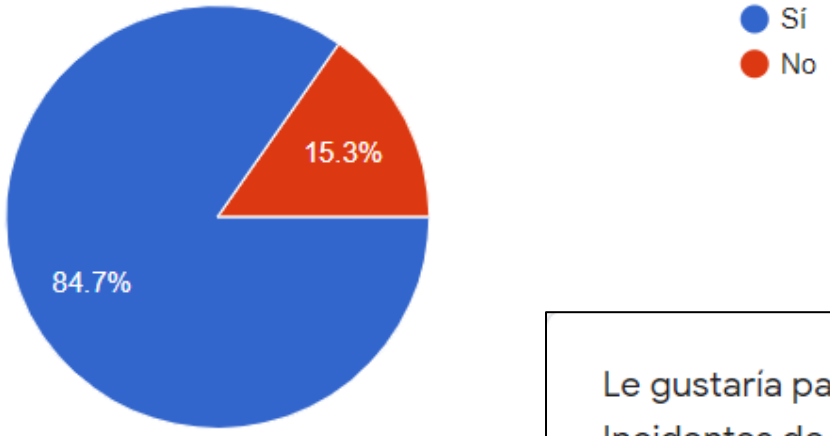
¿Qué tan importante es contar con convenios formales entre los CSIRT de las IES?

170 respuestas



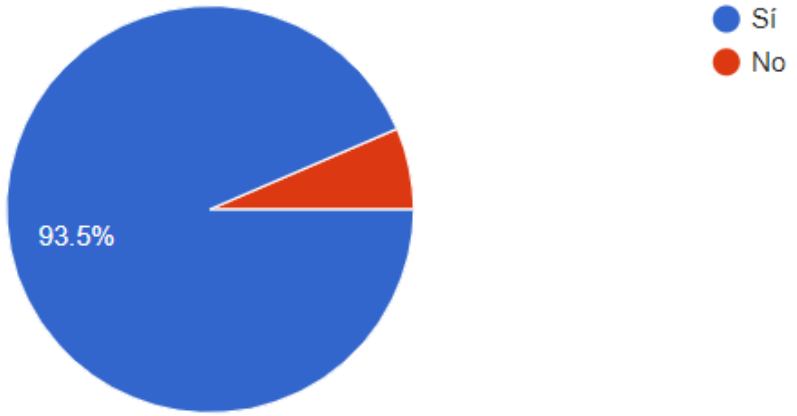
¿Le gustaría nombrar a algún representante de su institución para participar en las actividades del CSIRT de la Red Nacional de Educación e Investigación?

170 respuestas



Le gustaría participar en entrenamientos para la formación de Equipos de Respuesta a Incidentes de Seguridad en Cómputo (CSIRT)

170 respuestas



PROBLEMAS POR LA VELOCIDAD DE LOS CAMBIOS
Comentarios de los grupos de enfoque

- *"Se ha acelerado la rapidez con que aparecen nuevos riesgos y ataques"*
- *"Se necesitan soluciones cada vez más sofisticadas"*
- *"El teletrabajo, por el COVID, aceleró los riesgos. En el campus se tiene cierto control, pero al salir del campus los riesgos se incrementan y tenemos que proteger los equipos institucionales que salen a las casas, establecer conexiones seguras"*
- *"El repentino mayor uso de la nube complica los controles de seguridad"*

CONCLUSIONES

NO (%)	ACTIVIDAD
92.9	**Plan de certificación en ciberseguridad para directivos**
90.0	**Plan de certificación en ciberseguridad para personal operativo**
78.8	Implementado proceso de gestión y manejo de riesgos
75.1	Área de seguridad informática
69.4	Realiza pruebas de penetración al menos una vez al año
65.9	Plan de gestión de riesgos
64.0	Plan/proceso para recuperación de desastres
63.5	Programa de concientización para los usuarios
62.4	Realiza pruebas del código fuente
61.2	Realiza análisis de vulnerabilidad al menos una vez al año
60.6	NOC
57.1	Sistema de gestión de seguridad de la información
54.7	Realiza análisis de riesgo al menos una vez al año
52.4	Sistema de gestión de incidentes
51.2	Políticas de seguridad de la información
47.4	Sistema de seguridad para *endpoint*

Para todas las actividades mencionadas, en más del 50% de los casos NO se cuenta con ellas o NO se usan

PRINCIPALES PROBLEMAS QUE ENFRENTAN EN EL TRABAJO

PROBLEMA	TOP 2 BOX
Inversión en ciberseguridad se ve como gasto	68.8%
Falta de presupuesto	66.4%
Falta de recursos humanos	65.9%
Recursos humanos insuficientes	62.4%
Falta de normativas	45.8%

Presupuestos, recursos humanos y falta de normativas son los problemas más señalados

NECESIDADES DE COMUNICACIÓN Y COLABORACIÓN

ACTIVIDAD	%
Le gustaría participar en entrenamientos para la formación de Equipos de Respuesta a Incidentes de Seguridad en Cómputo (CSIRT)	93.5
Le gustaría nombrar a un representante para participar en las actividades del CSIRT de la Red Nacional de Educación e Investigación	84.7
Esta interesado en compartir experiencias en grupos/eventos organizados por las Redes Nacionales de Educación e Investigación Latinoamericanas	84.7
Es muy importante la comunicación, coordinación y apoyo entre las áreas de ciberseguridad de las IES	76.5
Es muy importante contar con convenios formales entre los CSIRT de las IES	68.8

GRACIAS