

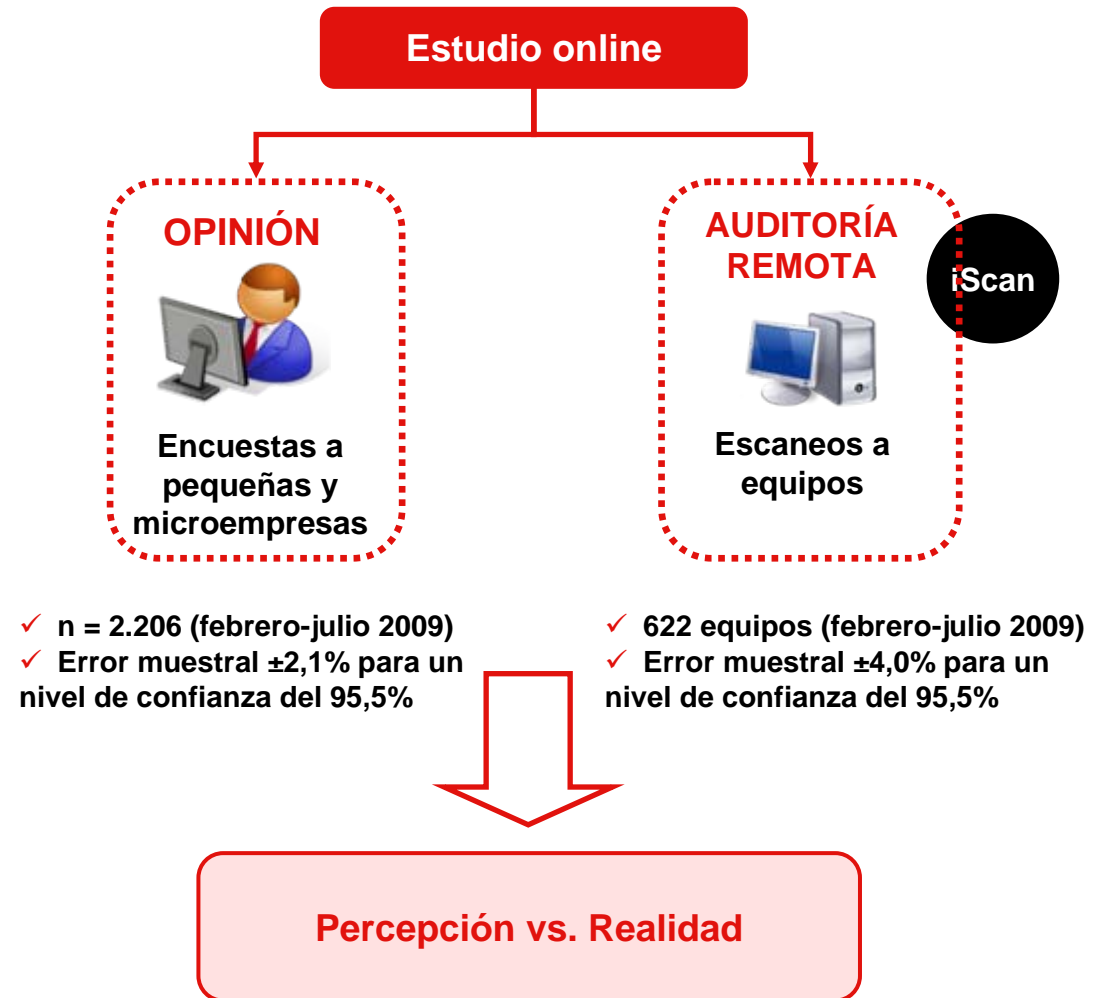
## Resumen ejecutivo del Estudio sobre la seguridad y e-confianza en las pequeñas y microempresas españolas



## OBJETIVOS DEL ESTUDIO

- ✓ **Contrastar** la **percepción** de seguridad de las pequeñas y microempresas españolas con la **situación real** de los equipos.
- ✓ Analizar el **grado de e-confianza** y **de seguridad** entre las empresas.
- ✓ **Orientar** iniciativas y **políticas públicas** para la mejora de la seguridad y la generación de un clima de confianza hacia la Sociedad de la Información

## METODOLOGÍA DEL ESTUDIO



## Universo

Empresas españolas de hasta 50 empleados, diferenciando entre las microempresas (menos de 10 empleados) y las pequeñas empresas (10-49 asalariados).

## Muestra

2.206 entidades y 622 equipos

## Distribución muestral

Muestreo aleatorio estratificado (número de empleados, sector de actividad y Comunidad Autónoma) con afijación proporcional según el porcentaje de uso de Internet.

## Captura de información

Página web creada para la difusión y participación en el estudio + Entrevistas online + Análisis en línea de los equipos

## Trabajo de campo

Febrero a Julio de 2009

## Error muestral

De acuerdo con los criterios del muestreo aleatorio simple en las que  $p=q=0,5$  y para un nivel de confianza del 95,5%, se establece un error muestral de  $\pm 2,1\%$  para  $n= 2.206$





- ❖ **Herramientas, buenas prácticas y políticas de seguridad**
- ❖ **Incidencias de seguridad**
- ❖ **Seguridad de las comunicaciones móviles e inalámbricas**
- ❖ **Consecuencias, reacciones y respuestas ante las incidencias de seguridad**
- ❖ **e-Confianza de las pequeñas y microempresas**
- ❖ **Sistema de indicadores de la seguridad de la información**

<http://observatorio.inteco.es>

- **Herramientas, buenas prácticas y políticas de seguridad.** Las empresas conscientes de la importancia de sus datos y de la información que albergan sus equipos, disponen de herramientas y/o soluciones a nivel de equipo y a nivel organización.
- Entre las herramientas implementadas en los equipos destacan por su grado de utilización los programas antivirus (97,8%), los cortafuegos (72,4%), los medios de control de acceso (66,8%) y los programas de anti correo basura (61%).
- Las principales medidas a nivel organizacional son el establecimiento de sistema de copias de seguridad de los datos (82,4%), los cortafuegos en red (72,9%) o los sistemas de prevención de intrusos (51,7%).
- Entre las buenas prácticas que se efectúan destaca la realización de copias de seguridad (por el 94,2% de las organizaciones) y la actualización de los programas y sistemas operativos (88,9%).
- La disposición de planes y políticas se refleja en la tenencia de un plan de seguridad (34,3%), de un plan de concienciación (17,6%) o de continuidad de negocio (11,9%).

- **Incidencias de seguridad.** El 48,4% de los equipos analizados tiene algún código malicioso o malware en junio de 2009. Se trata, en su mayor parte, de troyanos y adware, y se caracterizan por su alto nivel de diversificación y heterogeneidad.
- Confirmación del desconocimiento real de las empresas sobre lo que sucede en sus equipos en relación con la presencia de virus (el 42,9% cree haberlos sufrido mientras que la auditoria no ha identificado ninguno), de troyanos (la presencia real – 27,8% – supera el nivel percibido –21,7% –) y de software espía (el 15,1% de las empresas creen que lo tienen cuando en realidad está presente en el 1,4% de los equipos).
- **Consecuencias y reacción de las empresas ante las incidencias de seguridad.** El 77,4% afirma haber sufrido algún incidente de seguridad, lo cuál ha supuesto para el 54,9% la pérdida del tiempo de trabajo. Aún así, el 69% de las empresas afirma que no existe ningún tipo de impacto monetario sobre el negocio.
- **Conocimiento y adecuación a la normativa sobre protección de datos.** El 60,2% de las empresas reconocen estar afectadas por esta normativa. Además un 80% se sabe afectada por el hecho de disponer de ficheros con datos personales.
- **La e-confianza de las empresas españolas.** El 90,3% de las pequeñas empresas españolas afirma que les da confianza realizar operaciones bancarias online

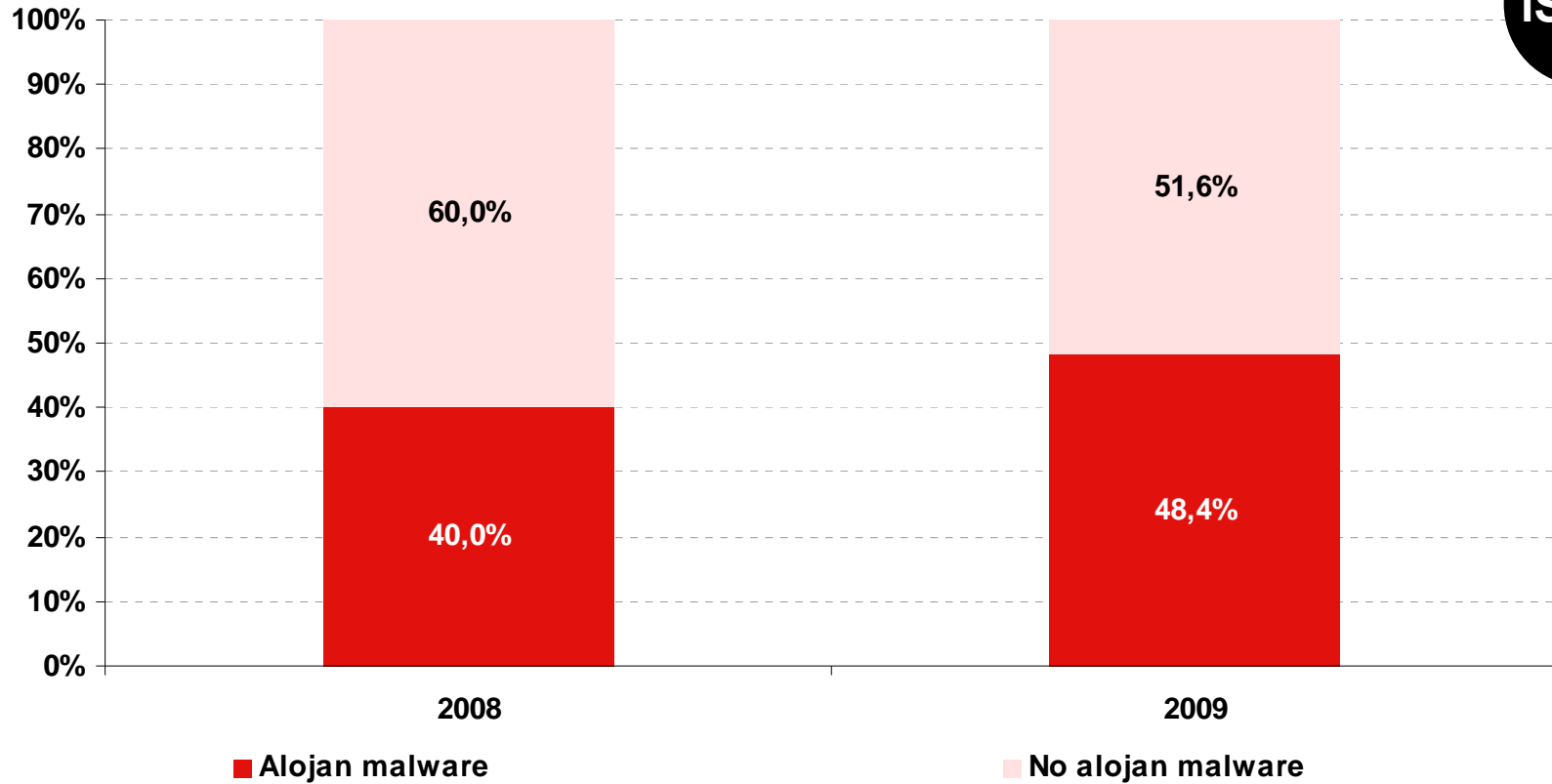
## Implantación de las soluciones de seguridad según el número de equipos en los que se encuentran instaladas (%)

Soluciones	En todos los equipos de la empresa	Sólo en determinados equipos
Programas de antivirus / anti-espía	94,7	3,1
Cortafuegos personal en los ordenadores	67,7	4,8
Medios de control de acceso/autenticación	61,3	5,5
Programas de anti correo basura	57,0	4,0
Herramientas de bloqueo de ventanas emergentes	50,1	4,3
Programas de limpieza de disco	39,4	4,2
Privilegios distintos en los equipos dependiendo del usuario	26,5	6,8
Herramientas que permitan acceso a su red desde fuera de la oficina	14,3	8,4
Herramientas de cifrado de disco	5,2	3,0

## Motivos declarados por las empresas para no utilizar las herramientas y soluciones de seguridad en los equipos (%)

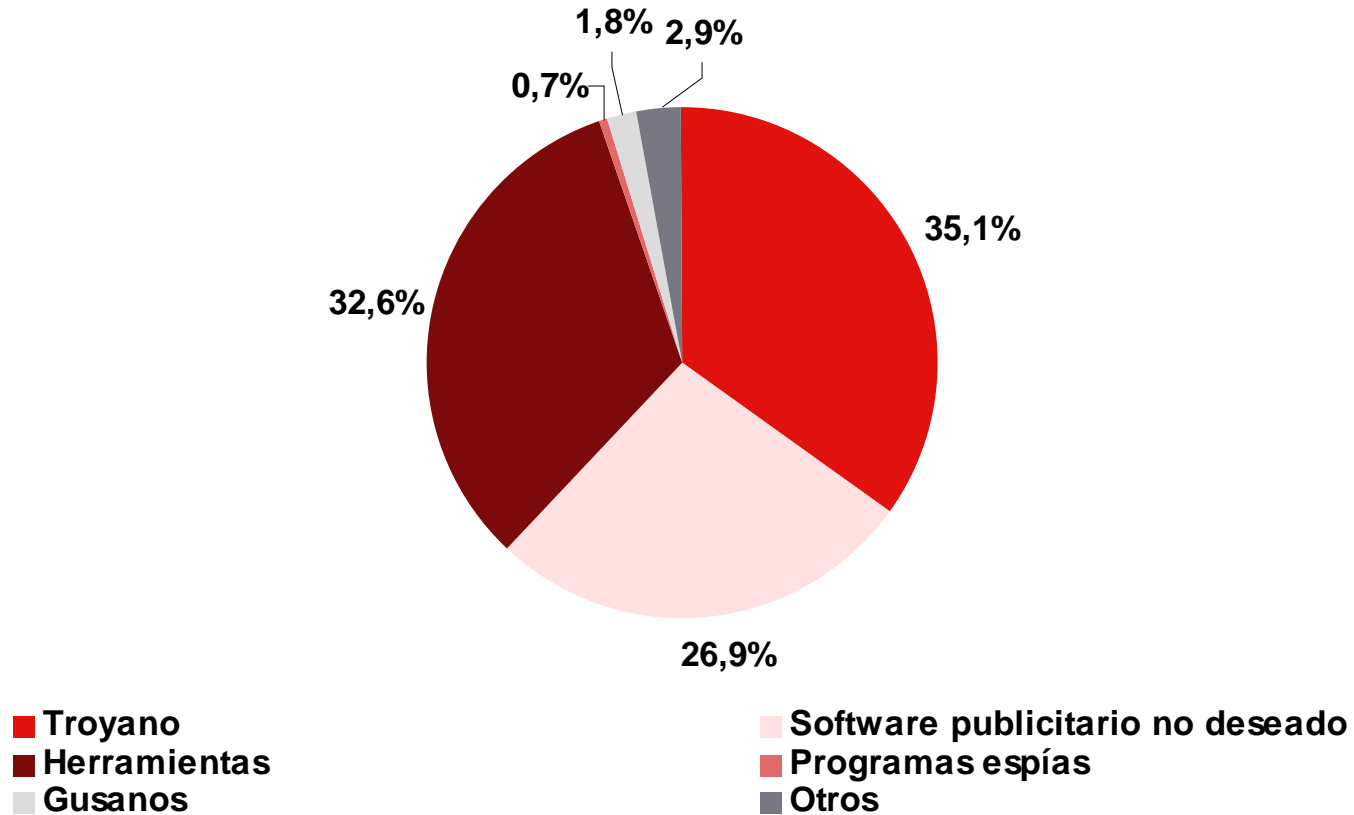
Soluciones	% Empresas que no lo utilizan	Motivos							
		No necesita	Precio	Entorpecen	Desconfía	Ineficaces	Otros	No conoce	No contesta
Programas de antivirus / anti-espía	2,2%	52,1	14,6	6,3	4,2	0,0	8,3	12,5	2,1
Cortafuegos personal en los ordenadores	27,6%	57,7	1,6	3,8	0,5	0,0	3,8	30,4	2,1
Herramientas de cifrado de disco	31,8%	66,2	0,9	1,1	0,3	0,6	1,5	28,1	1,2
Medios de control de acceso/ autenticación	33,2%	71,5	1,4	1,2	1,5	0,5	4,6	18,6	0,7
Programas de anti correo basura	39,0%	62,0	1,4	1,3	0,6	4,0	5,9	24,2	0,7
Herramientas de bloqueo de ventanas emergentes	45,6%	69,4	0,6	1,4	0,8	0,5	2,8	24,1	0,5
Programas de limpieza de disco	56,4%	64,5	0,7	1,3	0,6	1,4	2,3	28,4	0,8
Privilegios distintos en los equipos dependiendo del usuario	66,6%	75,4	0,5	1,1	0,7	0,7	2,6	18,0	1,1
Herramientas que permitan acceso a su red desde fuera de la oficina	77,3%	73,0	0,9	0,6	1,1	0,8	2,0	20,8	0,8

## Evolución anual del nivel de incidencias en los equipos de las empresas tras realizar la auditoria de seguridad (%)



2008 n=265; 2009 n= 622

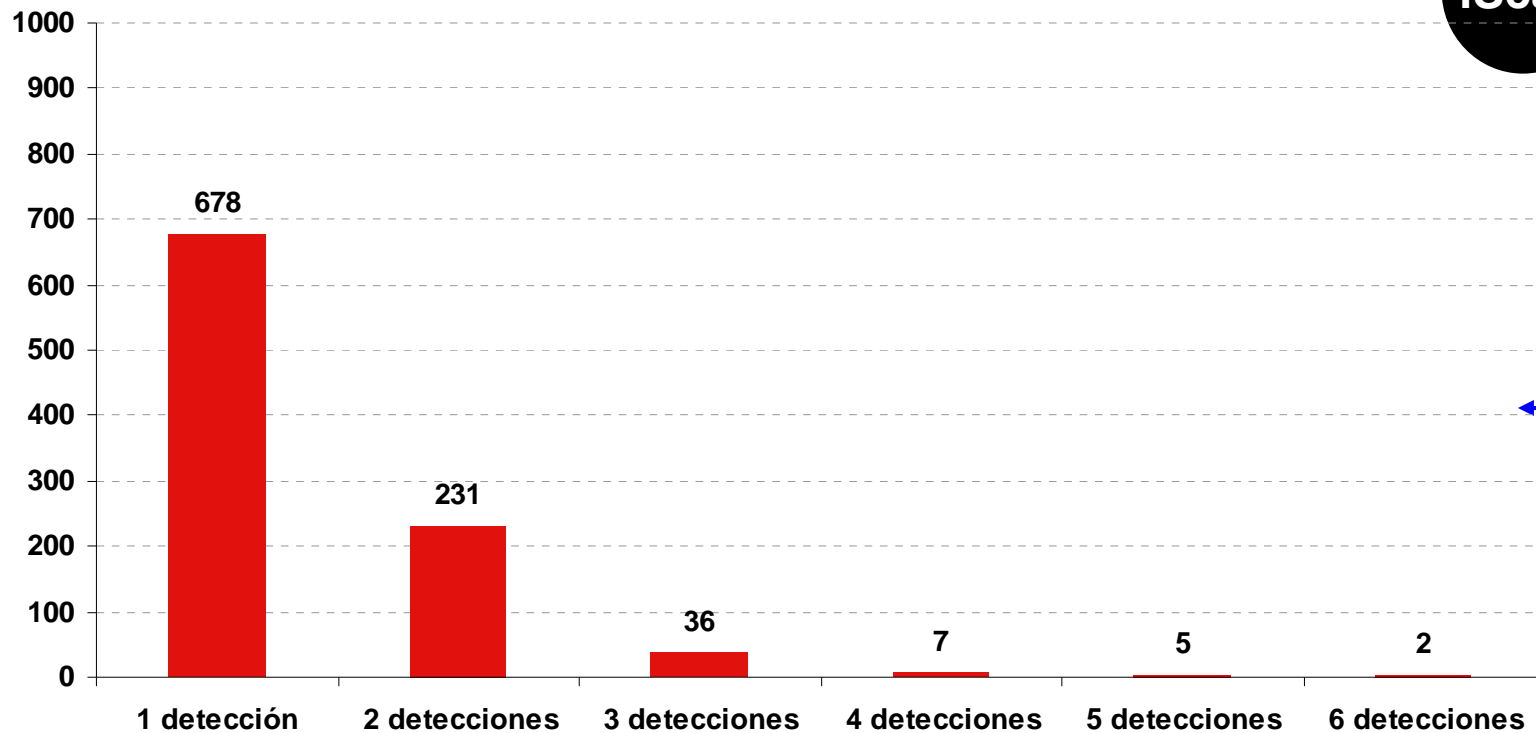
Distribución de las categorías de código malicioso (%)



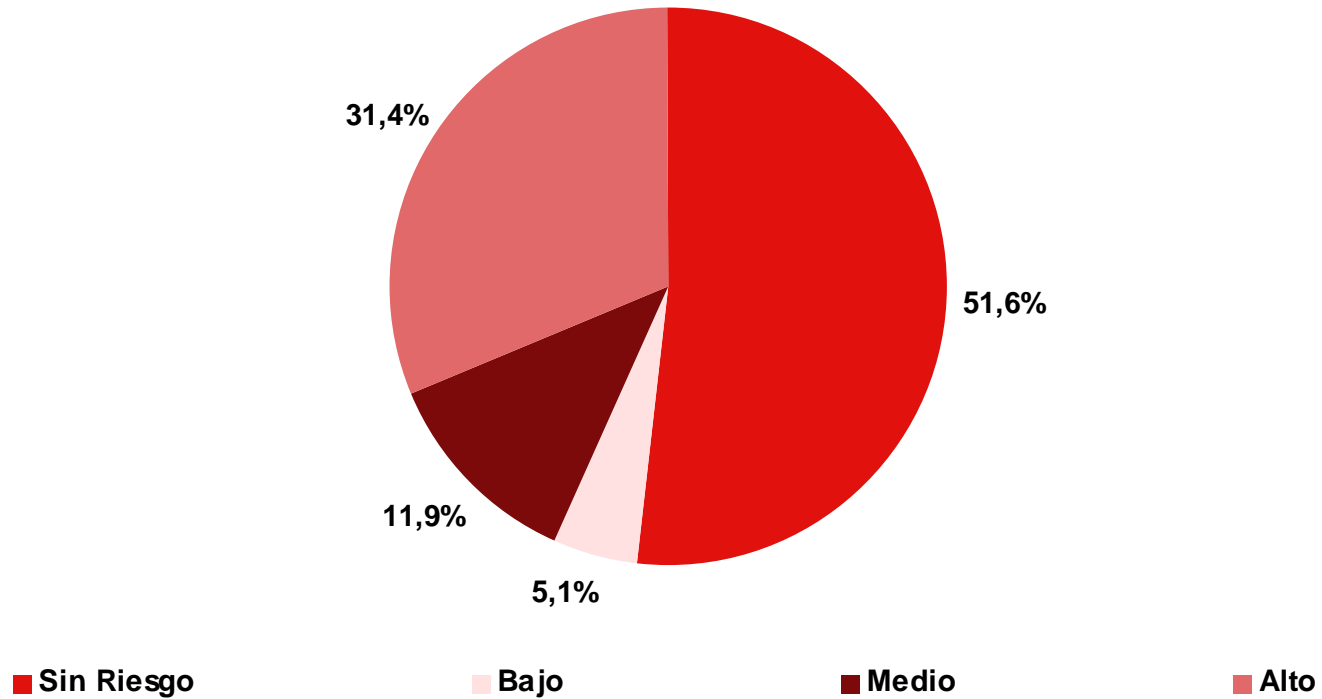
Número de variantes únicas de malware n=963

Variable analizada	Dato real
Número de archivos maliciosos	1.381
Variantes únicas de malware	963
<i>Índice de repetición de cada variante única de malware</i>	1,4

Número de detecciones de variantes únicas de código malicioso (may. 2009)

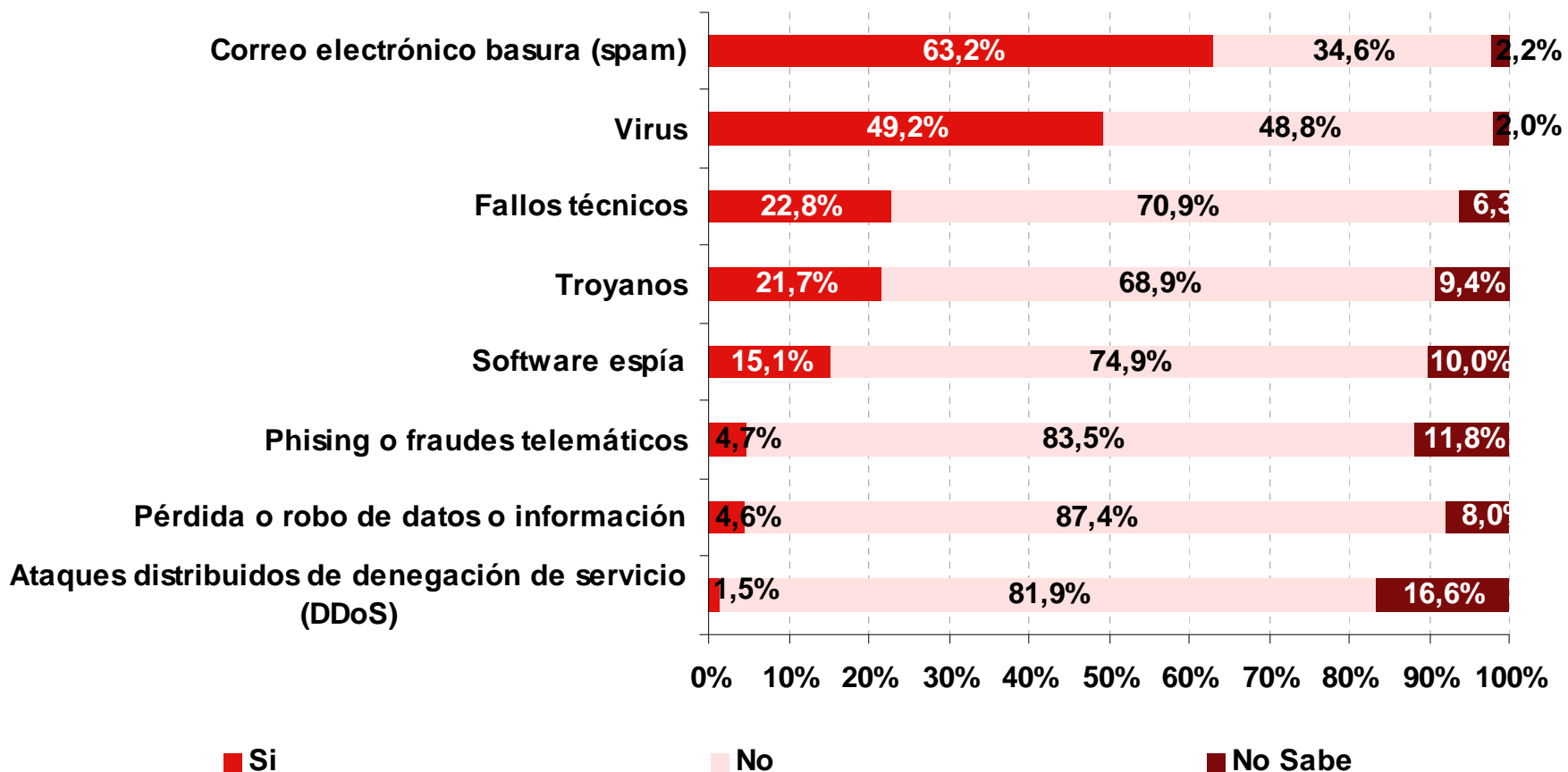


Distribución de los equipos en función del nivel de riesgo (%)



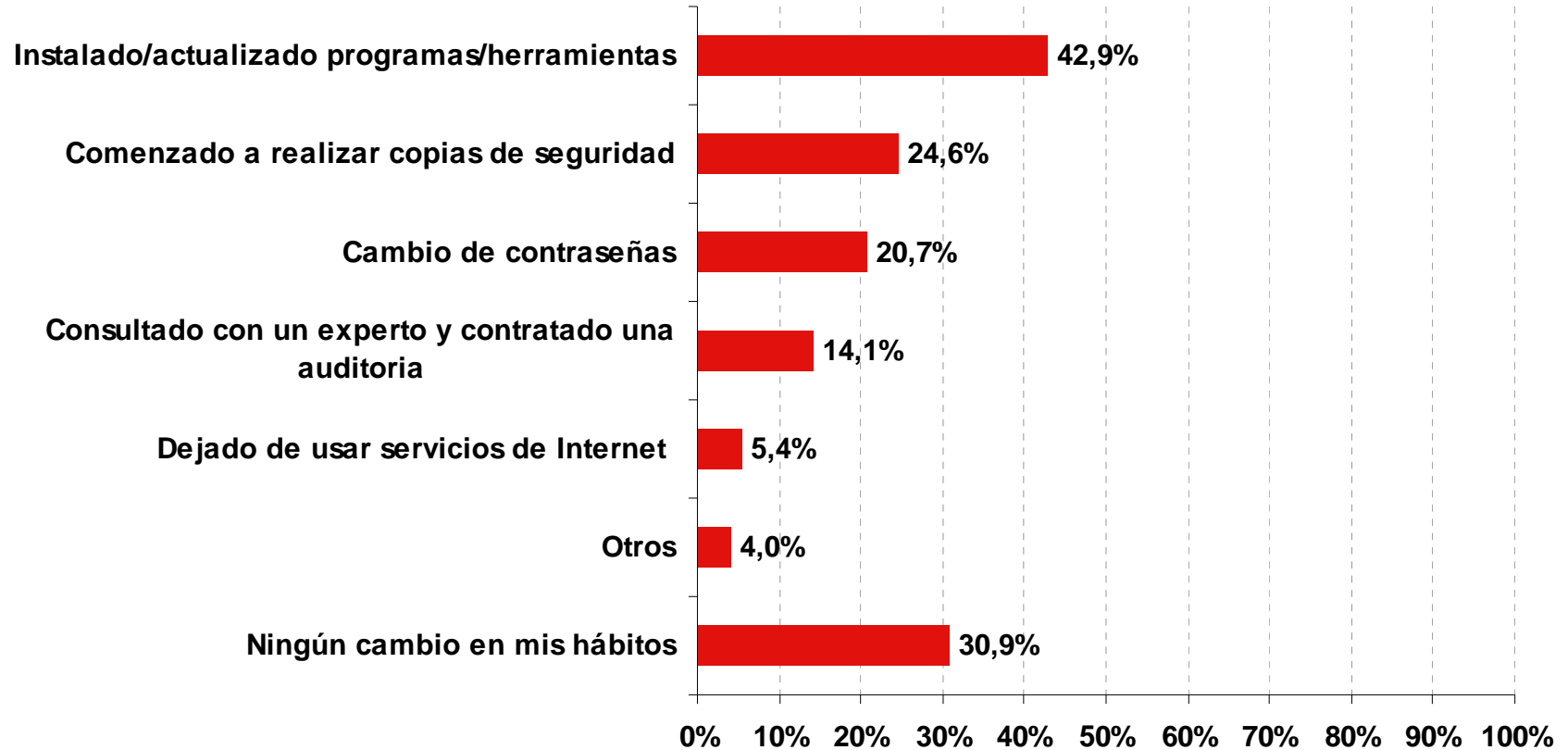
n=622

## Incidentes de seguridad declarados por las empresas (%)



n=2.206

## Cambios de hábitos en las empresas debido a un incidente de seguridad (%)



n=1.708

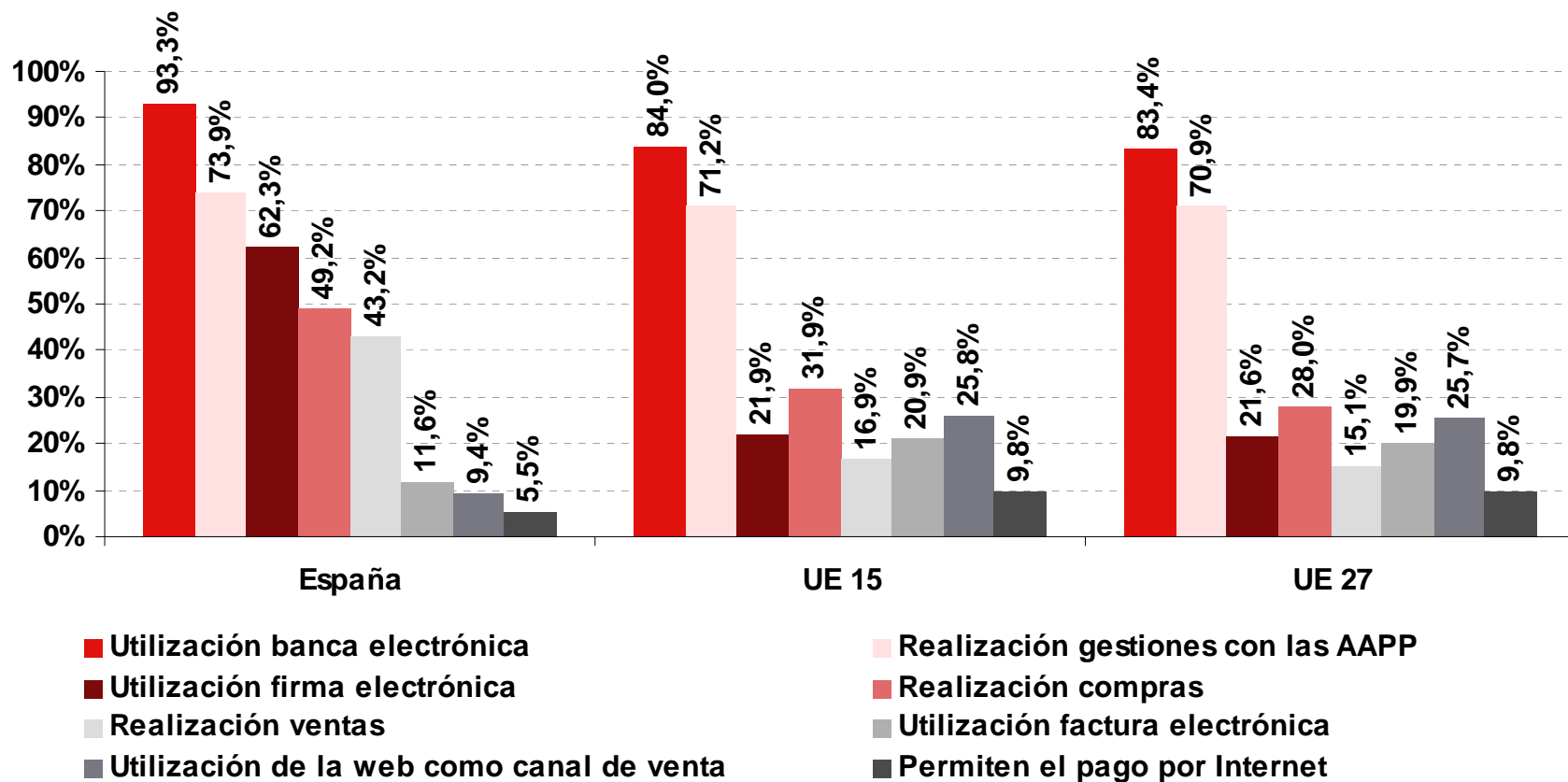
## Método empleado por las empresas para resolver incidentes (%)



n=1.708



## Comparativa europea según la utilización de servicios a través de Internet por parte de las empresas (%)



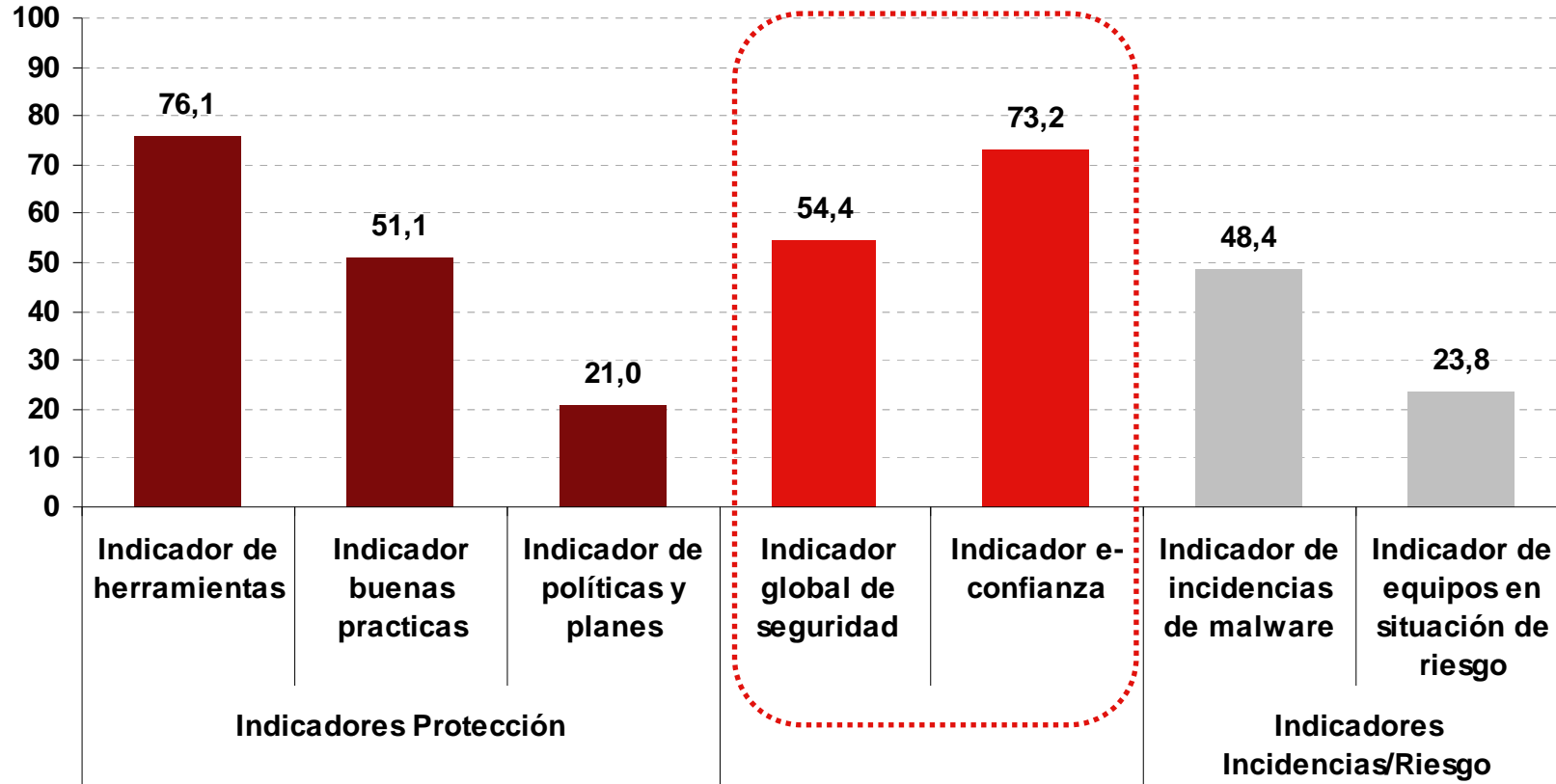
España n=329, Europa n=67.303

Grado de confianza de las empresas cuando realizan gestiones con la Administración Pública a través de Internet, según el tamaño de la empresa

Tamaño	% empresas que realizan	Confianza				
		Mucha	Bastante	Ni poca ni mucha	Poca	Ninguna
Menos de 10	54,3	39,4	50,5	6,6	2,2	1,3
De 10 a 49	73,8	41,7	48,8	6,3	2,4	0,8
<b>Total muestra</b>	<b>57,2</b>	<b>39,9</b>	<b>50,2</b>	<b>6,5</b>	<b>2,3</b>	<b>1,2</b>

n=1.261

## Sistema de indicadores de la seguridad de la información (0-100 puntos)



**INDICADORES DE PROTECCIÓN**

**INDICADORES DE INCIDENCIAS/RIESGO**

- ✓ El tamaño de la empresa es un condicionante a la hora de implementar las herramientas y soluciones de seguridad. Las pequeñas empresas presentan un porcentaje más elevado de instalación de casi todas las herramientas.
- ✓ Se demuestra que entre los empresarios existe una especial preocupación por la disponibilidad de su infraestructura tecnológica y la información que ésta soporta. Así la gran mayoría realiza copias de seguridad e instalan sistemas antivirus.
- ✓ Las pequeñas y microempresas españolas tienen la percepción de que la seguridad es un aspecto meramente tecnológico. Deben por consiguiente mejorar para poder incrementar sus niveles de seguridad y e-confianza.
- ✓ Además han de tomar conciencia de los riesgos que pueden existir, ya que un elevado porcentaje creen que no son susceptibles de sufrir un incidente de seguridad al considerarse “poco interesantes” para los posibles atacantes.
- ✓ Confusión y desconocimiento real de las empresas sobre lo que sucede en sus equipos en el tema de las incidencias de seguridad.
- ✓ Las herramientas de seguridad son necesarias pero no suficientes, y pueden provocar una falsa sensación de seguridad.
- ✓ Es importante que todos los implicados unan esfuerzos para evitar que los problemas de seguridad supongan un freno al desarrollo de la Sociedad de la Información.

	<b>FORTALEZAS</b>	<b>DEBILIDADES</b>
<b>Análisis Interno</b>	<ul style="list-style-type: none"> <li>✓ Buena capacidad tecnológica</li> <li>✓ Alto nivel de implantación de determinadas herramientas de seguridad.</li> <li>✓ Alto nivel de uso de la firma electrónica y otros servicios de Internet.</li> <li>✓ Creciente nivel de concienciación y adaptación en materia de protección de datos.</li> <li>✓ Alto nivel de e-confianza.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Existencia de vulnerabilidades, riesgos e impactos significativos.</li> <li>✓ Falsa sensación de seguridad.</li> <li>✓ Centradas en la dimensión tecnológica.</li> <li>✓ Lento progreso en algunos aspectos.</li> </ul>
	<b>OPORTUNIDADES</b>	<b>AMENAZAS</b>
<b>Análisis Externo</b>	<ul style="list-style-type: none"> <li>✓ Alto nivel de compromiso de las Administraciones Públicas y de las asociaciones de empresarios.</li> <li>✓ Enfoque de los fabricantes de productos de seguridad al mercado de seguridad de la información en las empresas.</li> <li>✓ Nivel de externalización de las funciones TI.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Lento progreso en seguridad que pudiera provocar una pérdida de competitividad.</li> <li>✓ Los dispositivos móviles e inalámbricos como potenciales brechas de seguridad para las empresas.</li> </ul>



Instituto Nacional  
de Tecnologías  
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>