La seguridad de la información y la e-confianza de los hogares españoles

Instituto Nacional de Tecnologías de la Comunicación

II Semana Seguridad Informática - Fundación Dédalo
Mesa redonda: "Internet, puerta abierta al mundo"
Tudela, 10 abril 2008.

Pablo Pérez San-José
Gerente del Observatorio (INTECO)

Observatorio de la Seguridad de la Información

¿Qué es INTECO?

Instituto Nacional de Tecnologías de la Comunicación (INTECO)

✓ Sociedad estatal promovida y adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

✓ Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, mediante la gestión, asesoramiento, promoción y difusión de proyectos asociados a las Tecnologías de la Información y la Comunicación (TIC).

✓ Tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

Líneas estratégicas de actuación de INTECO:

- **SEGURIDAD**
- **Accesibilidad**
- **Innovación TIC**
- **Ciudadanía e Internet**
- **e-Salud**

Observatorio de la Seguridad de la Información

✓ El **Observatorio de la Seguridad de la Información** se inserta dentro de la línea estratégica de actuación de INTECO en materia de seguridad y e-confianza.

✓ Su misión es **describir de manera detallada y sistemática** el nivel de seguridad y confianza en la Sociedad de la Información en los hogares, empresas y administraciones, así como **generar conocimiento divulgativo y especializado** en la materia.

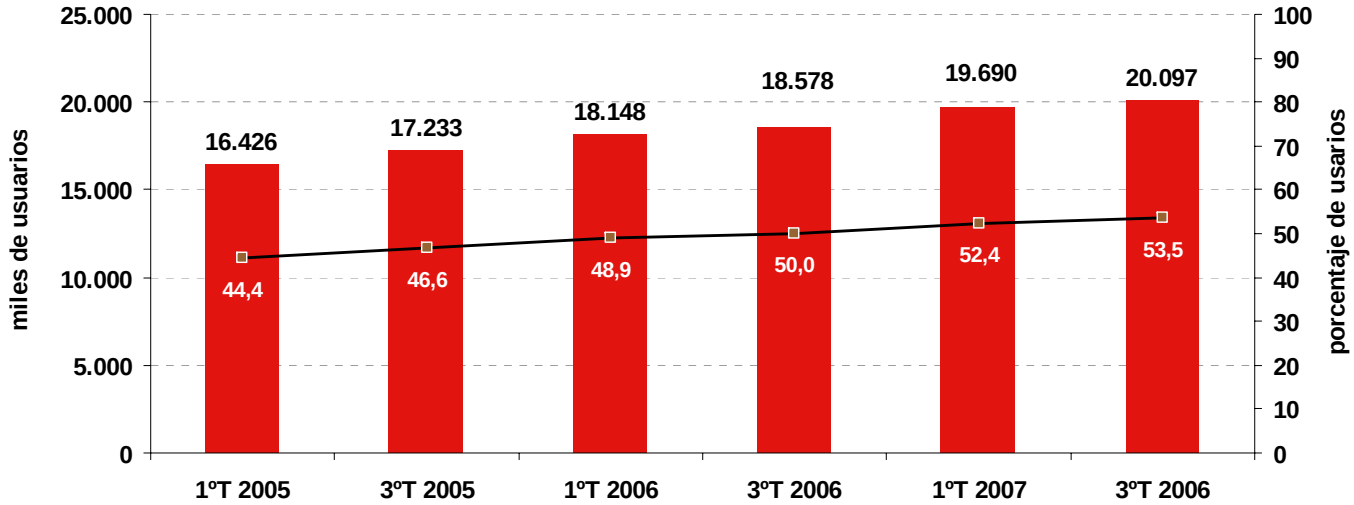
✓ Se basa en dos pilares fundamentales:

- **Métrica**
- **Análisis y diagnóstico**

¿Por qué es necesario medir la seguridad?

- ✓ **Internet es un fenómeno masivo: más 50% población lo usa.**

Evolución del uso de Internet (en miles de personas)



- ✓ **Lagunas y falta de información en seguridad de la información.**
- ✓ **Cierto alarmismo en las medios de comunicación**

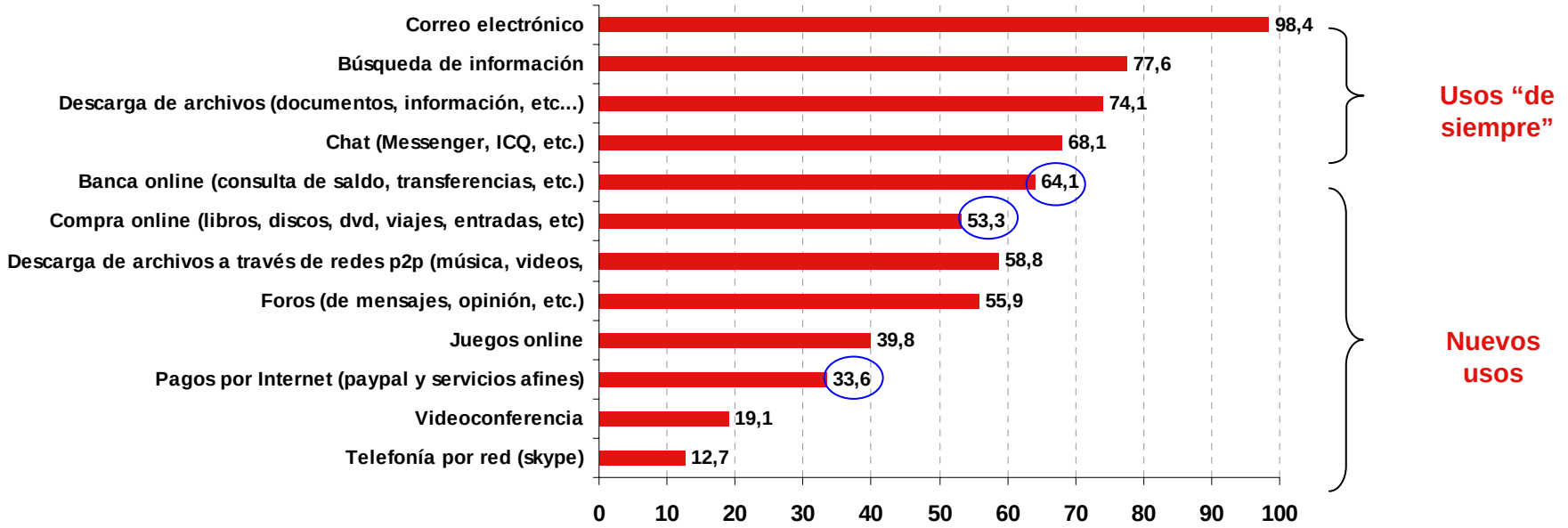
Es necesario describir y analizar rigurosamente, generar conocimiento especializado y difundir la cultura de la seguridad a través de la información, formación y sensibilización a los usuarios

¿Por qué es necesario medir la seguridad?

Uso mayoritario de Internet

- Avance, no sólo de los usos sociales de Internet (chat, correo, blogs), sino también de los usos económicos (banca online, comercio electrónico, juegos).
- El correo electrónico es utilizado por la práctica totalidad de los individuos.
- 6 de cada 10 usuarios usan redes P2P para transferir archivos.
- 4 de cada 10 juegan online.

Servicios y usos de Internet



Proyectos de Investigación del Observatorio

Ciudadanos:

- ✓ **Estudio sobre la seguridad de la información y e-confianza de los hogares españoles.**
- ✓ **Estudio sobre los hábitos de seguridad en el uso de las TIC y acceso a contenidos por niños y adolescentes y la e-confianza de padres y tutores.**
- ✓ **Estudio sobre usuarios y profesionales de entidades públicas y privadas afectadas por la práctica fraudulenta conocida como *phishing*.**
- ✓ **Estudio sobre la situación, naturaleza e impacto económico del correo electrónico no deseado (spam).**

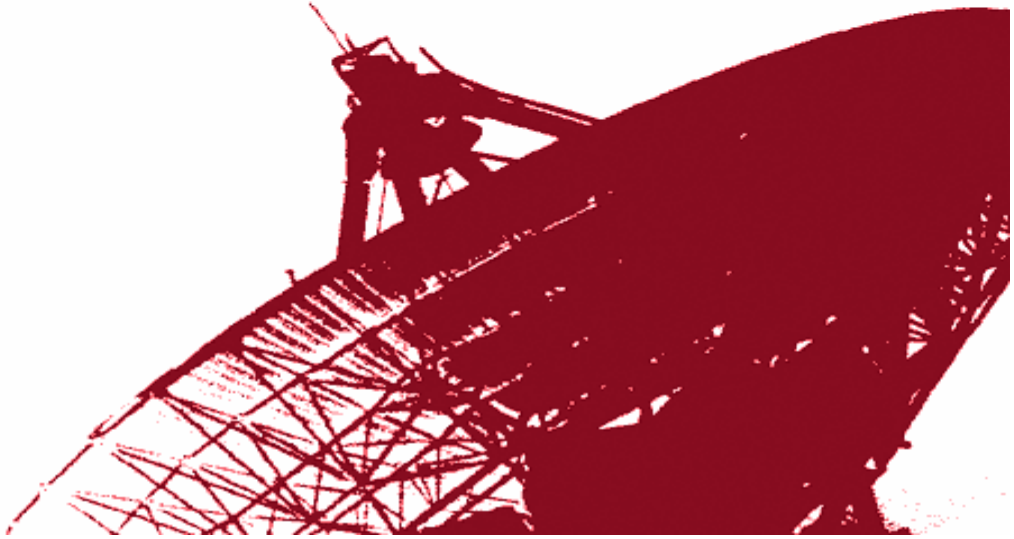
Empresas:

- ✓ Estudio sobre incidencias y necesidades de seguridad en las Pequeñas y Medianas Empresas españolas.
- ✓ Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento (RLOPD).
- ✓ Estudio sobre el sector de la seguridad TIC en España.
- ✓ Estudio sobre la situación de seguridad y buenas prácticas en los dispositivos móviles y las redes inalámbricas.
- ✓ Estudio sobre medidas de seguridad en plataformas educativas.

Administraciones Públicas:

- ✓ Estudio sobre la seguridad de la información y e-confianza en el ámbito de las Entidades Locales.
- ✓ Estudio sobre las iniciativas para la promoción y difusión de la e-confianza y seguridad de la información por parte de las Comunidades Autónomas.
- ✓ Estudio sobre la seguridad de los datos de carácter personal en el ámbito de las Entidades Locales españolas y su grado de adaptación a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento (RLOPD).

Estudio sobre la seguridad de la información y e-confianza de los hogares españoles



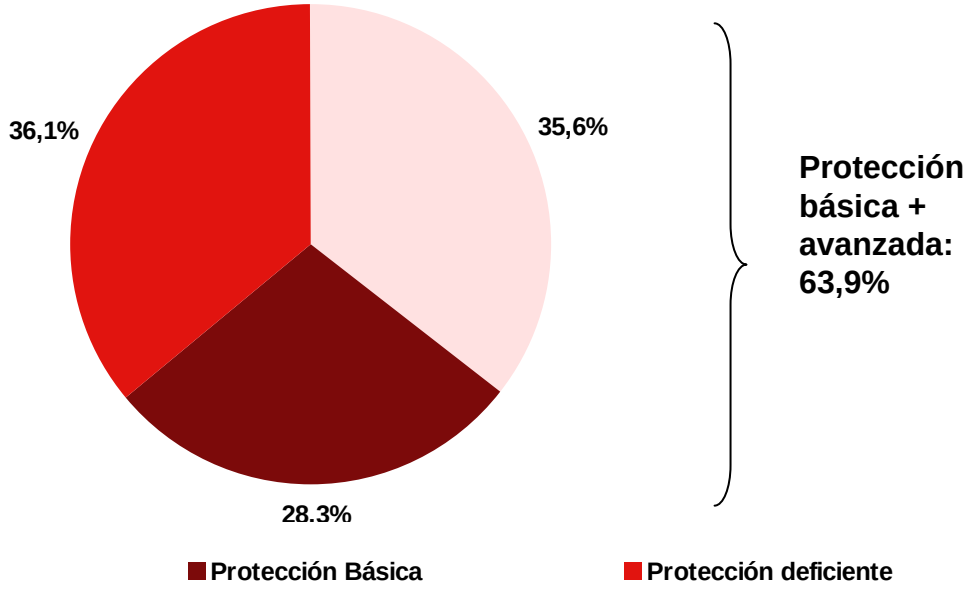
Medidas y herramientas de seguridad

✓ Podemos diferenciar las herramientas y medidas de seguridad según el nivel de participación del usuario en: **automatizables** (medidas pasivas) y **no automatizables** (medidas activas).

✓ En principio, el 64% de los ordenadores de los hogares españoles está razonablemente protegido (**básicas + avanzadas**).

- **Protección Avanzada:** Declaran utilizar tanto protección proactiva como automatizable.
- **Protección Básica.** Fundamentalmente medidas automatizables.
- **Protección Deficiente.** Presentan niveles muy bajos en ambos tipos de protección.

Grado de protección de los equipos de los hogares



Medidas y herramientas de seguridad

- ✓ Las medidas más generalizadas siguen siendo antivirus y cortafuegos, frente a medidas como copias de seguridad o contraseñas seguras.
- ✓ Los usuarios utilizan fundamentalmente medidas de seguridad automatizadas, es decir, aquellas que no implican interacción por parte del usuario.

Medidas de seguridad %	Dispone en Enero	Dispone en Abril
Programas antivirus	94,4	93,3
Cortafuegos o *firewalls*	65,3	72,4
Bloqueo de ventanas emergentes	61,5	65,5
Eliminación de archivos temporales y *cookies*	55,2	58,5
Programas anti-correo basura o *anti-spam*	49,9	52,0
Programas anti-espía o *anti-spy*	49,0	51,9
Actualizaciones de seguridad del SO	45,8	47,8
Contraseñas (acceso equipos y documentos)	44,9	47,2
Copias de seguridad de archivos importantes	28,5	32,0
Partición del disco duro	27,3	30,8
Copia de seguridad del disco de arranque	18,6	21,9
Encriptación de documentos	6,9	7,9
Programas de control parental	7,9	7,7
Ninguna de las mencionadas	0,4	1,2

Medidas y herramientas de seguridad

- Las **principales razones para no incorporar las medidas de seguridad** son:
  - Desconocimiento.
  - Percepción de que ésta es innecesaria.
  - Porque consideran que entorpece el uso del ordenador y la navegación por Internet.

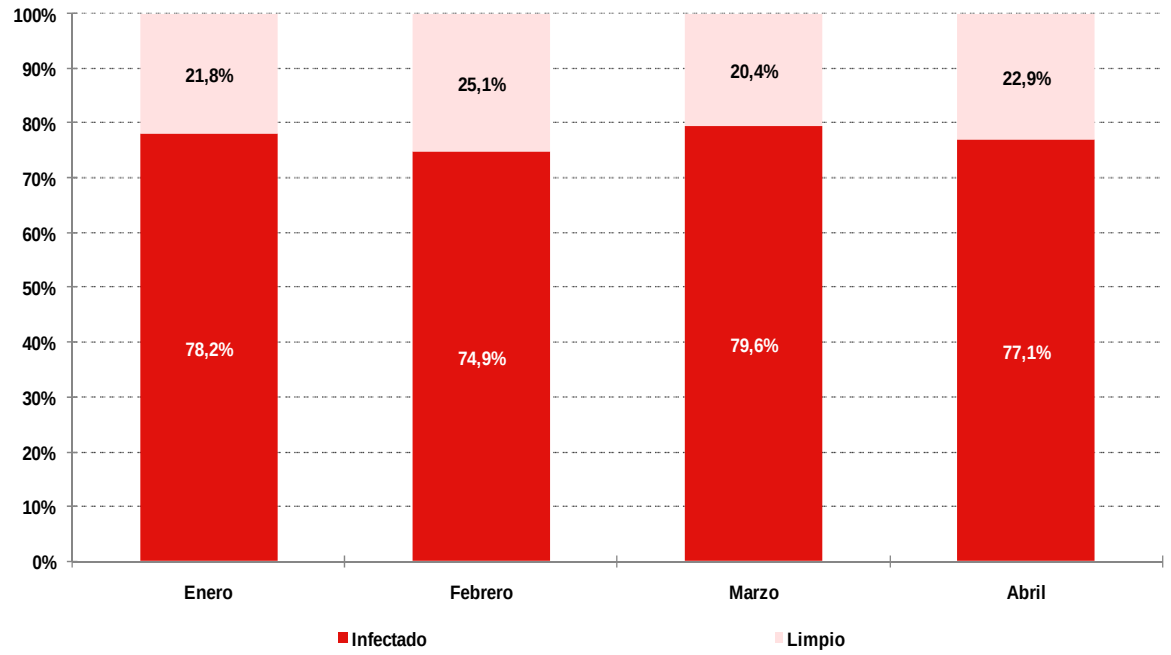
Medidas de seguridad	No sé lo que es	Porque es innecesario	Precio	Entorpecen	Desconfío	Ineficaces
Programas antivirus	7,1	17,0	16,7	43,1	5,1	11,0
Cortafuegos o *firewalls*	25,8	31,3	7,9	27,4	3,9	3,7
Programas de ventanas emergentes	20,6	38,3	9,4	17,9	5,3	8,5
Programas anti-espía o *anti-spy*	19,5	32,0	11,8	17,9	9,9	8,9
Programas anti-correo basura o *anti-spam*	11,8	44,7	12,5	13,9	5,1	12,0
Actualizaciones de seguridad S.O.	18,6	48,0	10,4	12,5	4,7	5,8
Eliminación de archivos temporales y/o *cookies*	16,3	59,0	5,8	9,8	3,1	6,0
Partición del disco duro	22,3	58,4	4,3	8,4	2,7	3,9
Contraseñas (acceso equipos y documentos)	8,2	72,1	3,7	7,8	3,6	4,6
Copias de seguridad de los archivos más importantes	11,0	67,9	6,1	7,0	3,0	5,0
Encriptación de documentos	25,7	58,2	5,0	6,3	2,7	2,1
Programas de control parental	8,6	76,5	3,8	5,8	1,9	3,4
Copia de seguridad del disco de arranque	16,6	66,2	4,7	5,7	2,7	4,1

Incidencias de seguridad

8 de cada 10 ordenadores domésticos para acceso a Internet presentan algún tipo de código malicioso (malware).

✓Se ha detectado **malware con riesgo alto** en el 58% de los equipos analizados.

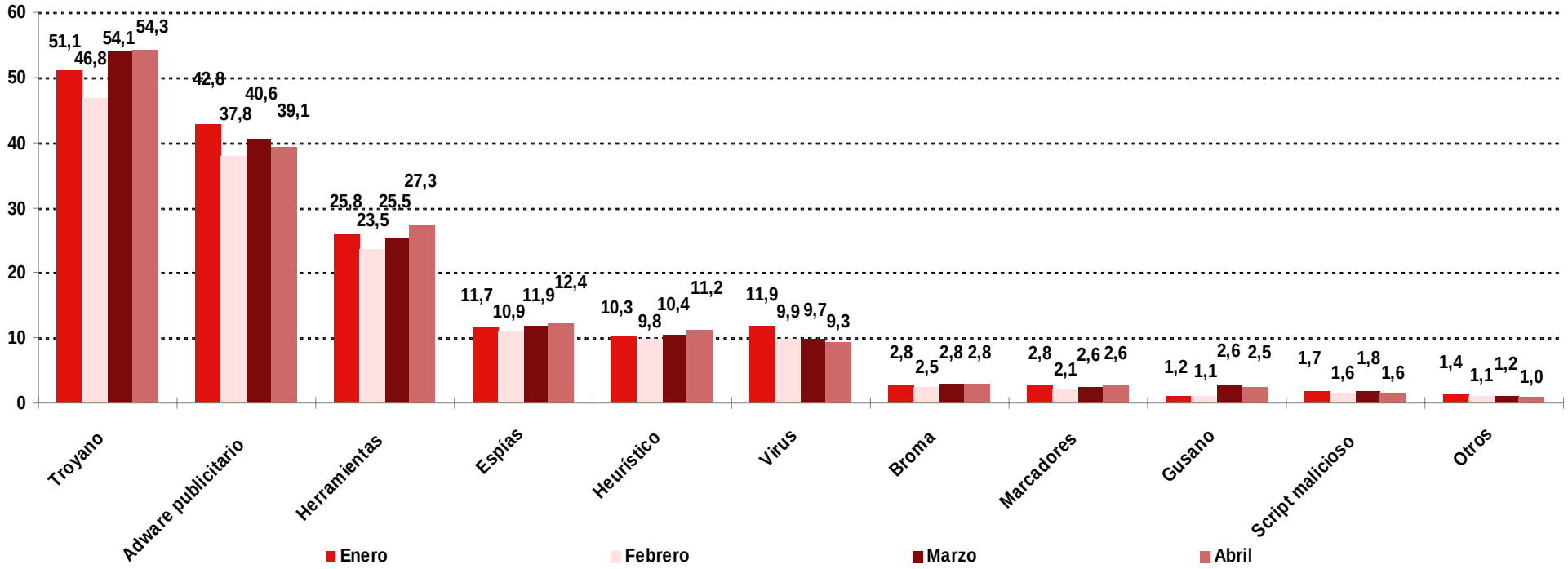
Evolución del malware detectado



Incidencias de seguridad

- En algo **más del 50% de los ordenadores** domésticos analizados se ha detectado la presencia de troyanos y casi en el 40%, adware publicitario.
- Menos del 10% de las detecciones son virus.

Presencia de malware por categorías (% sobre el total de ordenadores escaneados)



Incidencias de seguridad

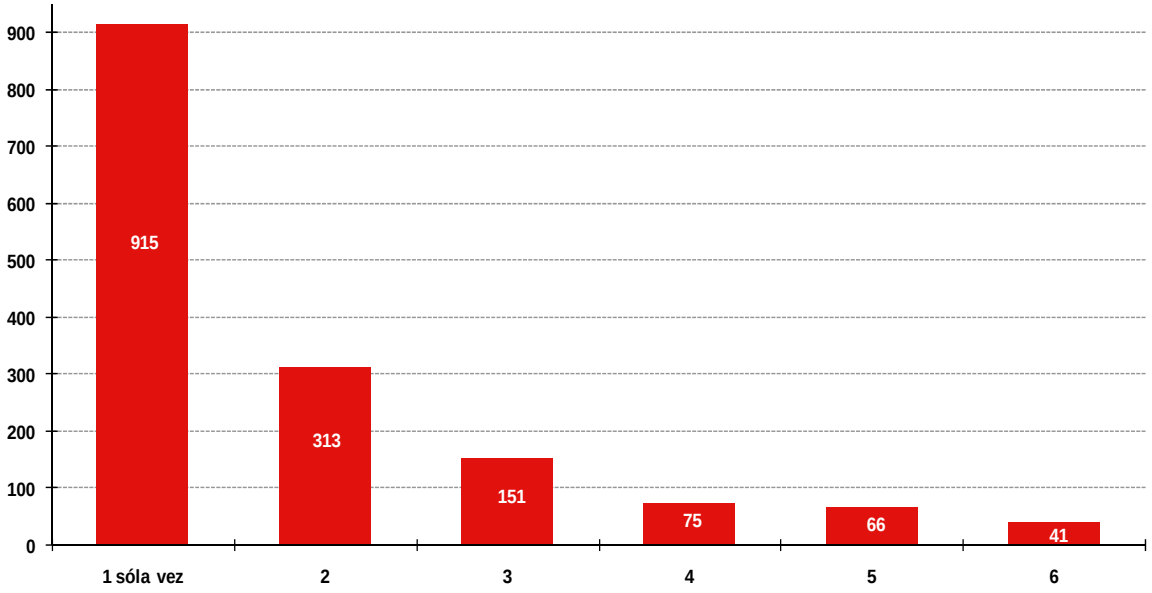
- ✓ Alta diversificación del malware que hace más difícil su detección y prevención.
- ✓ De entre el malware encontrado aquel que genera un mayor **<u>número de variantes</u>** distintas son los troyanos (50%); son virus tan solo el 0,7% de las variantes únicas.

Amenazas silenciosas

Los usuarios no siempre son conscientes de la presencia de malware porque actualmente los desarrolladores de estos códigos tienen el objetivo de que sus creaciones pasen desapercibidas

- ➢ <u>Antes:</u> **Notoriedad**.
- ➢ <u>Ahora:</u> **Explotación de información sensible con fines lucrativos/delictivos; utilización de capacidad y ancho banda de terceros con fines espurios.**

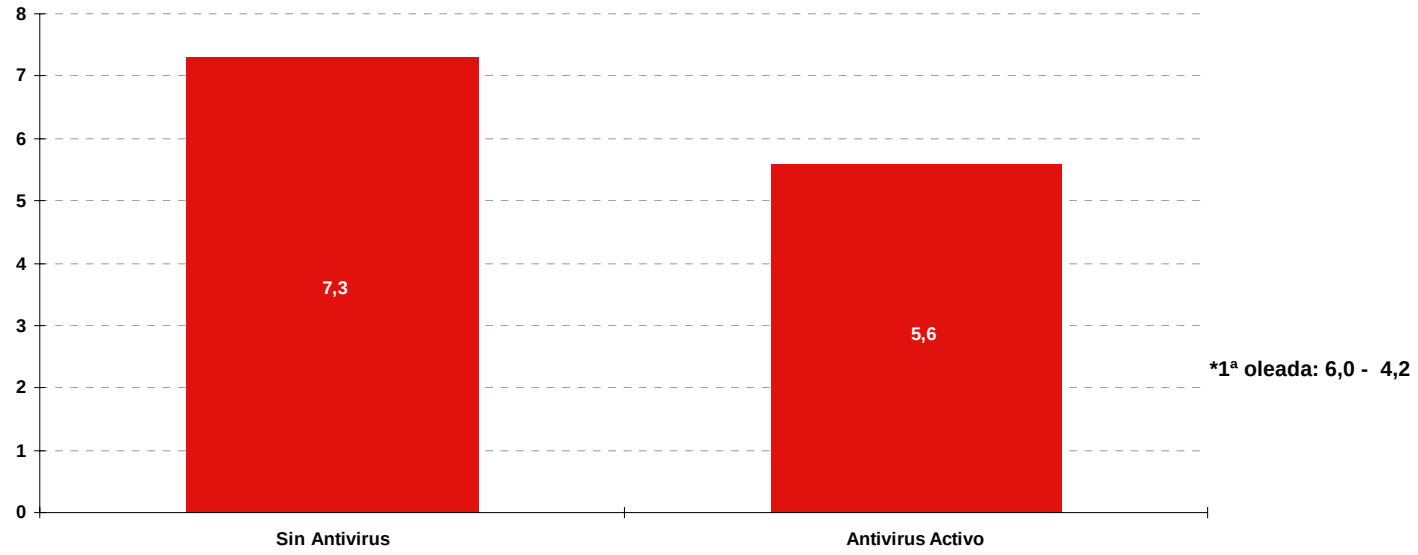
Número de detecciones de cada código malicioso



La seguridad en Internet no es sólo una cuestión de máquinas y tecnología, sino de personas

1er motivo: herramientas no son suficientes

Número medio de archivos infectados en función del uso de antivirus



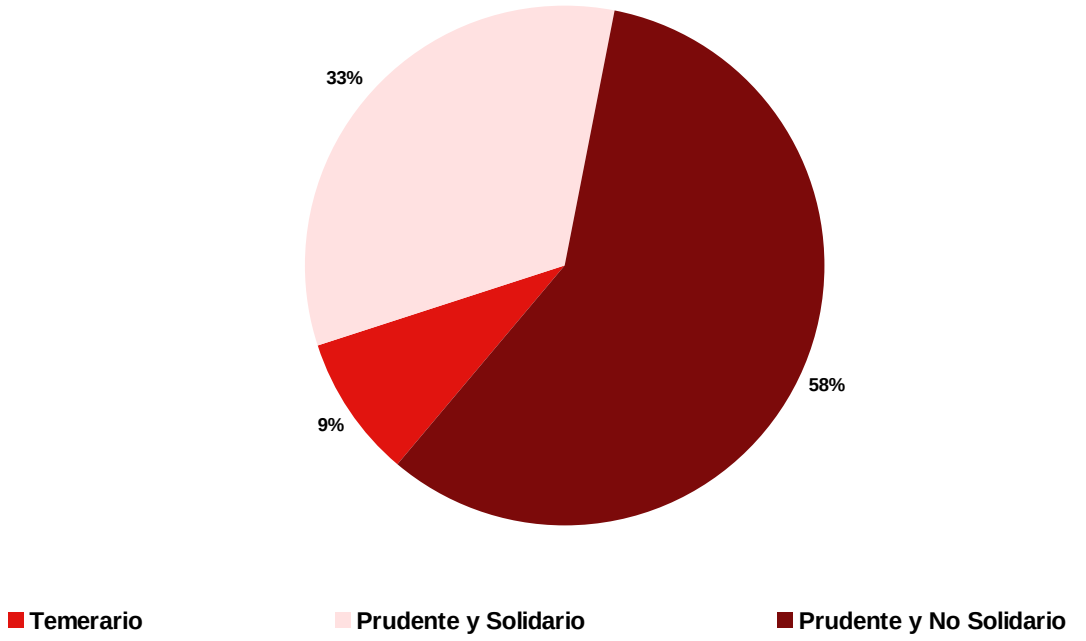
- ✓ Se constata que **la instalación de un antivirus es necesaria pero no es suficiente**.
- ✓ Además es preciso aplicar otras medidas: buenas prácticas y hábitos de uso basados en la responsabilidad, la precaución y la protección.

2º motivo: temeridad concentrada en unos pocos usuarios

✓El riesgo tiende a concentrarse en el reducido grupo (± 10%) de usuarios imprudentes: los llamados “temerarios”

- ✓ **Prudente y no solidario**. Tiene un enfoque individualista de la seguridad. Se centra en la defensa del equipo particular y no comparte experiencias para la defensa solidaria.
- ✓ **Prudente y solidario**. Añade a la protección individual la preocupación por compartir y la mutua ayuda en temas de seguridad.
- ✓ **Temerario:** No atiende a las normas y hábitos básicos de la prudencia. No modifica sus hábitos a pesar de sufrir incidencias de gravedad.

Distribución de los usuarios por grupos según hábitos de uso



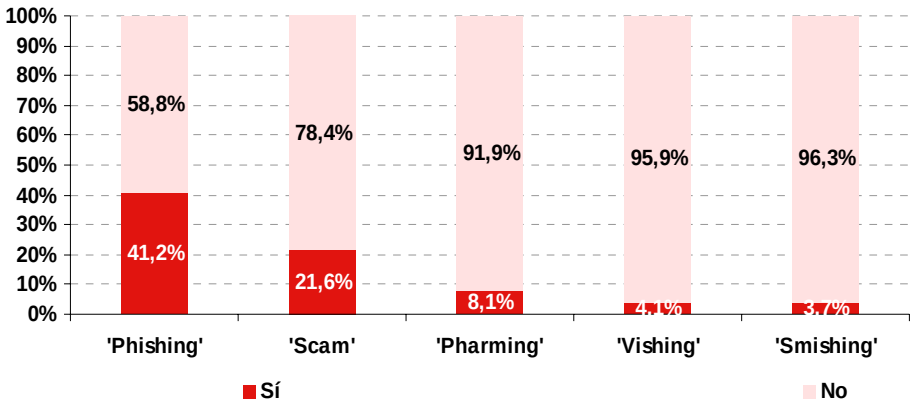
Fuente: INTECO

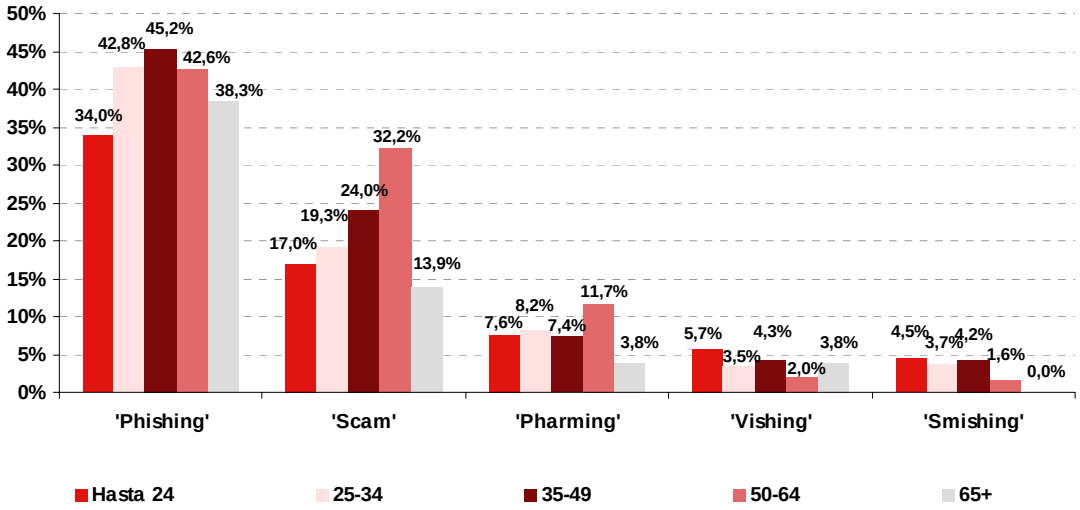
Incidencias de seguridad

3er motivo: lenguaje poco adaptado al usuario

✓ En muchas ocasiones la nomenclatura que utiliza el sector bien por ser **muy técnico** o bien por basarse **en otros idiomas** provoca que el usuario medio no la asocie a las incidencias que sí son conocidas por él.

¿Conoce el significado de alguno de los siguientes términos?





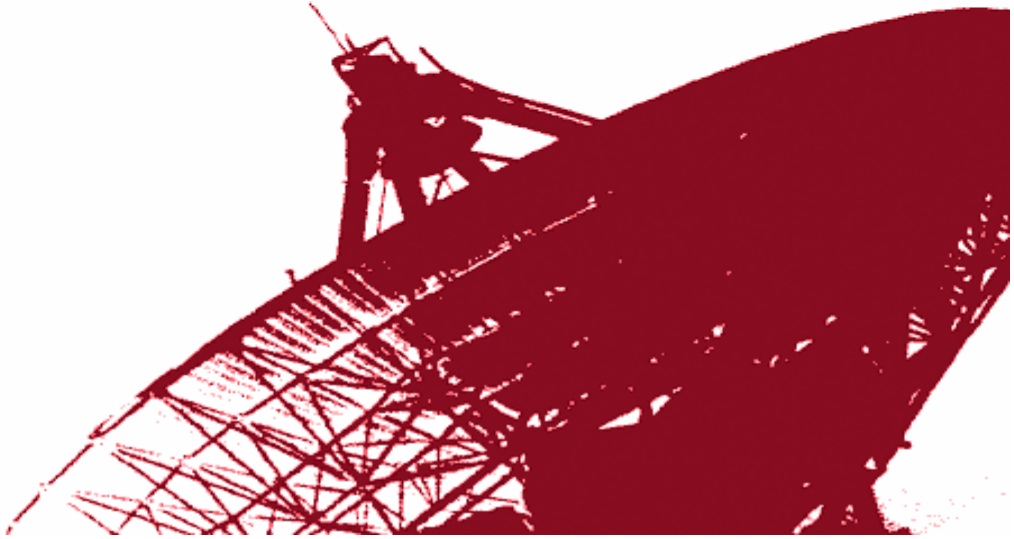
El papel de la Administración: tutelaje vs. autorregulación

La mayor parte de los ciudadanos piensan que para mejorar la seguridad hay que **combinar las medidas preventivas individuales con una acción más decidida por parte de las Administraciones Públicas** que ayude a limitar las incidencias de seguridad.

- ✓ Los **usuarios piden a la Administración** que:
  - Controle y vigile más de cerca lo que está pasando en Internet.
  - Que informe y/o alerte a los usuarios.
  - Que sea más diligente en la persecución de delitos o prácticas abusivas.

- ✓ **¿Cuál es el impacto de los problemas de seguridad en el desarrollo de la Sociedad de la Información?**

Estudio sobre usuarios y profesionales de entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing.



Fraude online: ¿qué es el phishing?

✓El phishing es una forma de ataque, en la que el delincuente, suplanta la identidad de una organización conocida (banco, organismo o empresa) a través de medios telemáticos (correo electrónico, mensajes sms, llamadas telefónicas, webs falsas).

- Fenómeno en permanente **evolución**: smishing (sms), vishing (llamada telefónica), pharming (redireccionamiento a web falsa)
- **Afecta** a un variado y **heterogéneo grupo de agentes**: bancos, subastas y comercio electrónico (eBay, Amazon, Myspace), organismos públicos (INE, AEAT), donaciones ONGs.

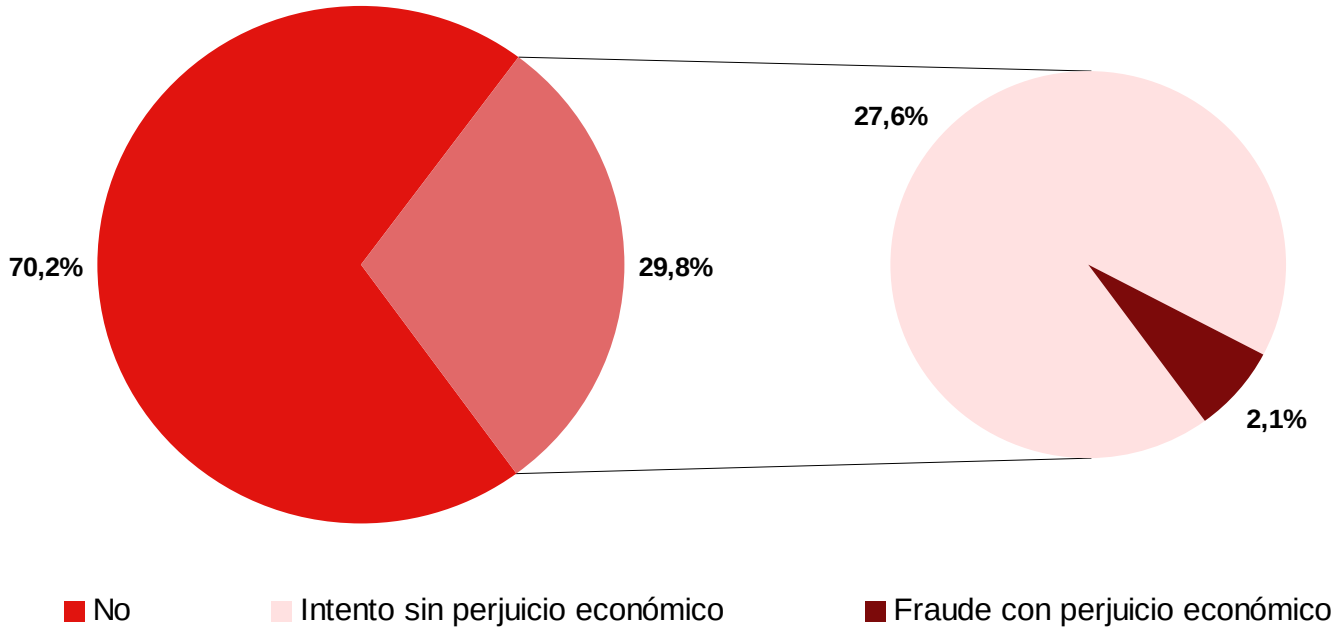
El phishing no es más que una reformulación de las estafas tradicionales a Internet.

Fraude online: Incidencias

✓El **29,9%** de los usuarios habituales de Internet, declaran haber sufrido algún **intento de fraude online.**

✓Un **2,1%** de los usuarios han sido objeto de un intento de **fraude con perjuicio económico**.

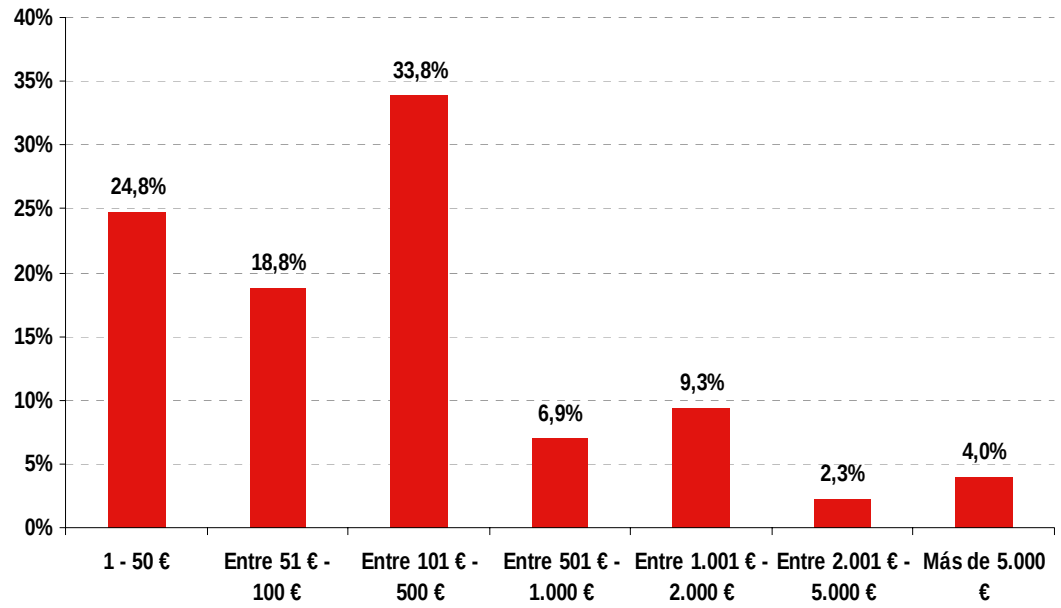
Porcentaje de usuarios que han recibido algún intento de fraude online y porcentaje de usuarios que han sufrido un perjuicio económico



Fraude online: Impacto social y económico

- ✓ **En algo más de 2 de cada 3 fraudes el perjuicio económico no supera los 400€ (límite entre delito y falta en el Código penal).**
- ✓ **Freno de la Sociedad de la Información y un freno de la economía basada en transacciones electrónicas.**

Porcentaje de usuarios que han sufrido fraude online según perjuicio económico soportado. (%)



No osbtante, la e-confianza se mantiene alta

Fraude online: Recomendaciones

HÁBITOS SEGUROS

- ✓ Sea precavido
- ✓ Sospeche de mensajes en otros idiomas
- ✓ Realice transacciones con un ordenador de confianza (mejor no público)
- ✓ Contraseñas seguras y no compartidas
- ✓ Teclee la dirección web del banco
- ✓ Su entidad bancaria jamás le solicitará su clave/s por correo electrónico. Nunca facilite esta/s a terceros por teléfono o fax.
- ✓ Compruebe certificados y conexión

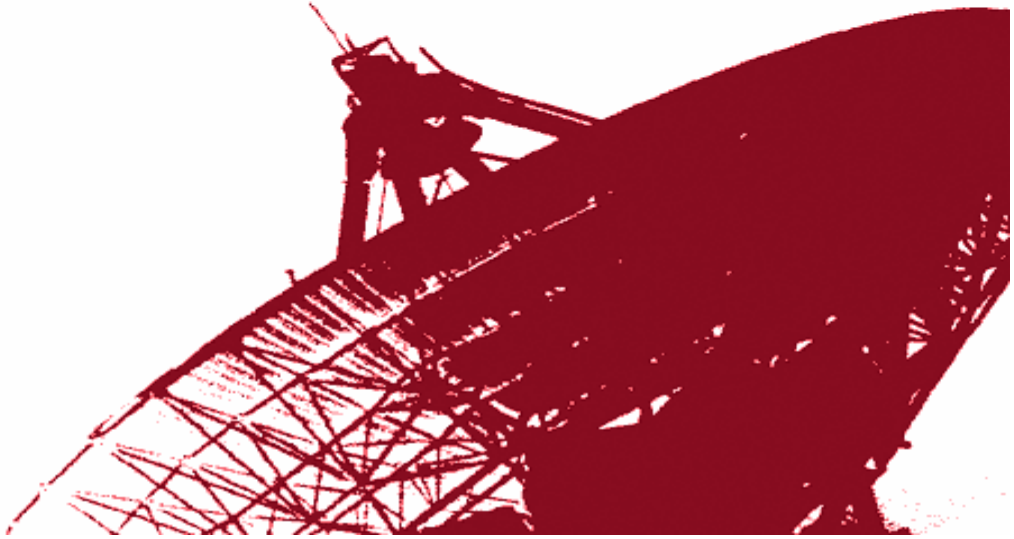
HERRAMIENTAS

- ✓ Mantenga su equipo protegido: actualice navegador y antivirus e instale parches de seguridad de sus programas
- ✓ Herramientas anti-phishing
- ✓ DNI electrónico y/o tarjetas de coordenadas

En caso de resultar afectado por un fraude online: DENUNCIE

- El **sector bancario** en España está adoptando un **comportamiento ejemplar**: una vez conocen que un cliente ha sufrido una estafa en su cuenta a través de Internet, están asumiendo el coste que conlleva el daño producido.
- Las **FCSE** vigilan, investigan, persiguen y responden.

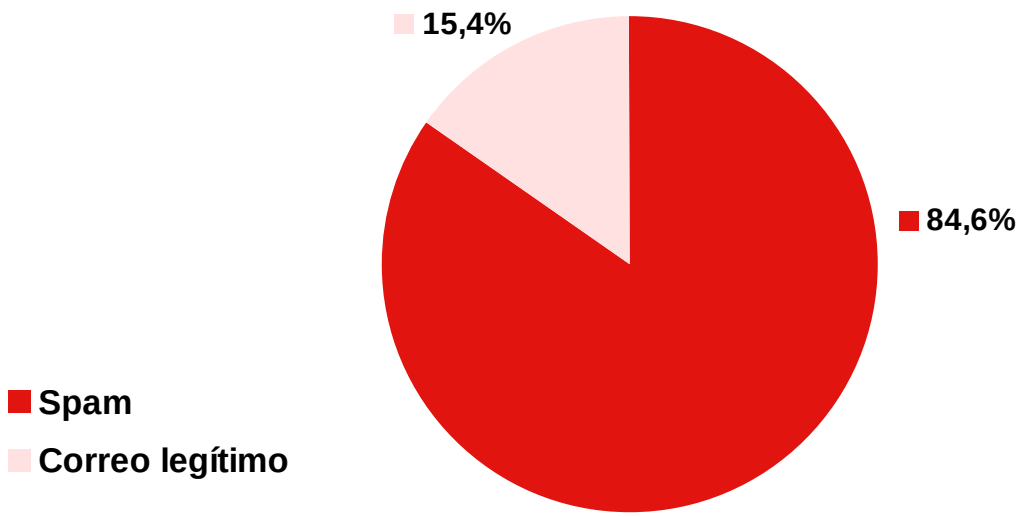
Estudio sobre la situación, naturaleza e impacto económico del spam



¿Qué es el spam?

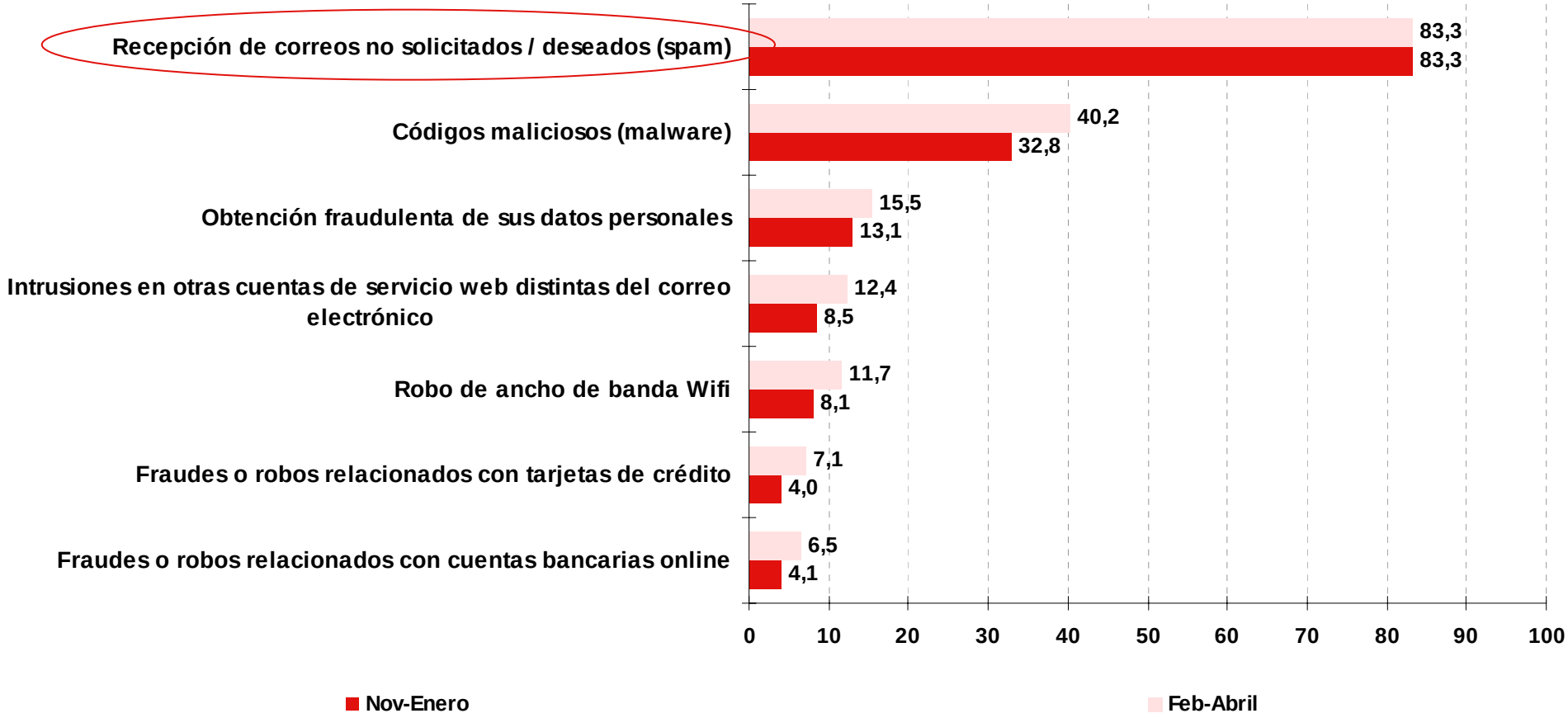
- El spam puede defirnirse como *"correo electrónico masivo no deseado"* o bien como aquellos correos publicitarios no autorizados que recibimos.
- Actualmente 3 de cada 4 correos que circulan por el mundo son s*pam.*

Distribución de *spam* en España (1/1/08 a 11/3/08 (%)



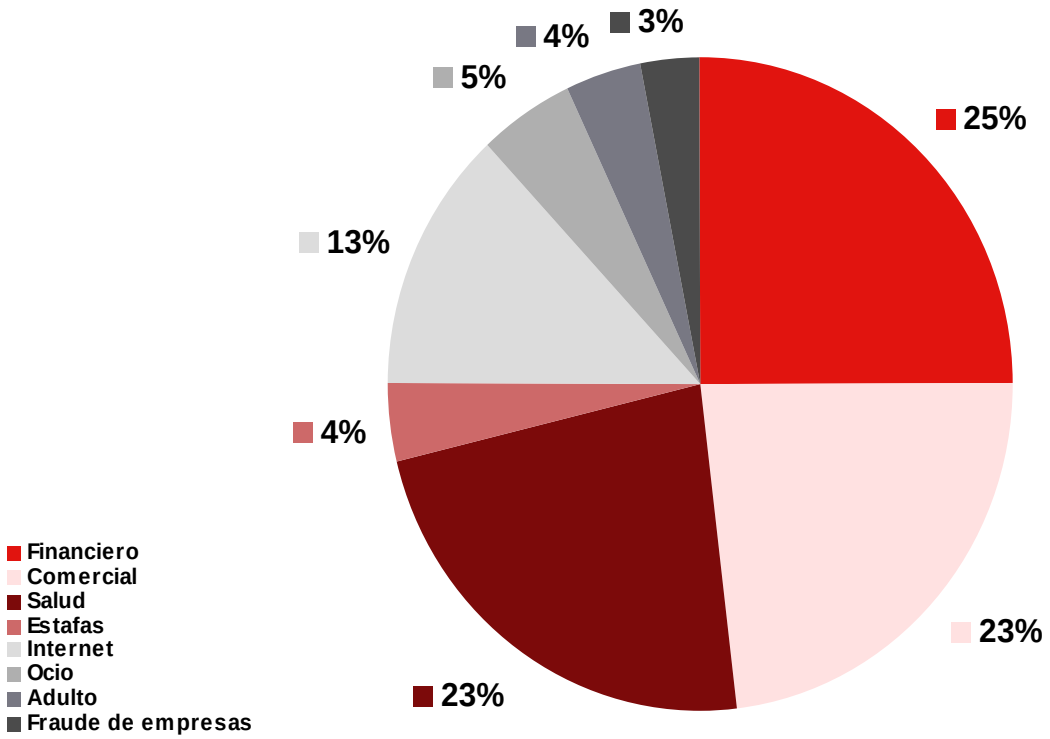
Incidencia del spam

Porcentaje de incidentes de seguridad en los ordenadores domésticos



Temática del spam

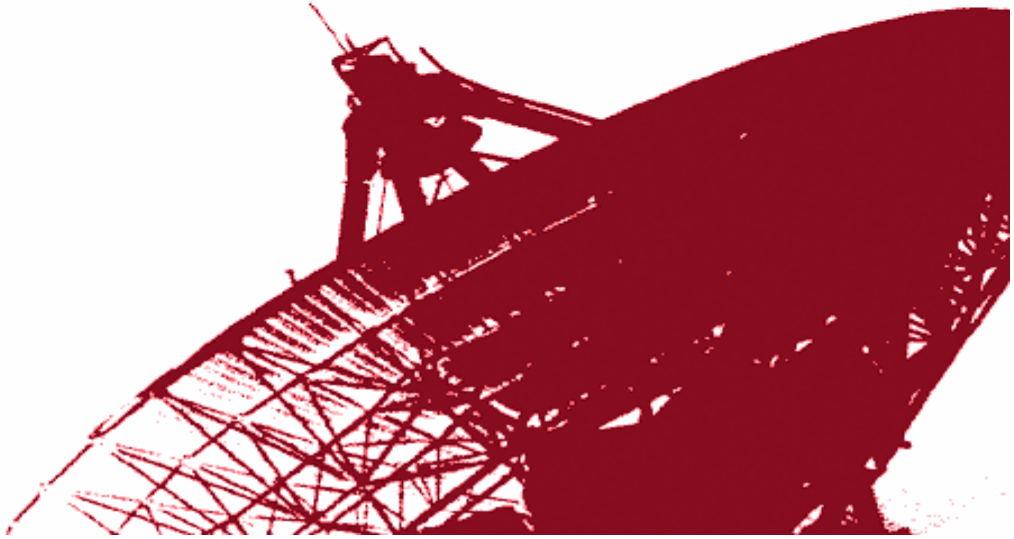
Distribución de tipos de spam en febrero del 2007 (%)



Recomendaciones a los usuarios para evitar el spam

- ✓Desconfiar de los correos que prometen interesantes beneficios.
- ✓Nunca responder a un correo electrónico no deseado por muy realista que parezca.
- ✓Nunca solicitar ser eliminado de una lista de distribución de correo en la cual no se ha inscrito.
- ✓Cuando se envía un correo a una lista de direcciones conocidas, utilizar la copia oculta.
- ✓Nunca visitar, o hacerlo con extrema precaución, direcciones Web recibidas o incluidas en correos electrónicos.
- ✓No publicitar su cuenta de correo de manera directa en Internet.
- ✓Utilización de varias cuentas de correo electrónico y empleo de éstas en su entorno adecuado (laboral, personal, ocio)
- ✓Es indispensable mantener su ordenador protegido, con los antivirus actualizados, con cortafuegos y filtros de spam que detecten intentos de conexión no autorizados.
- ✓Mantener siempre activas las herramientas de filtro antispam.

Estudio sobre los hábitos de seguridad en el uso de las TIC de niños y e-confianza de padres y tutores.

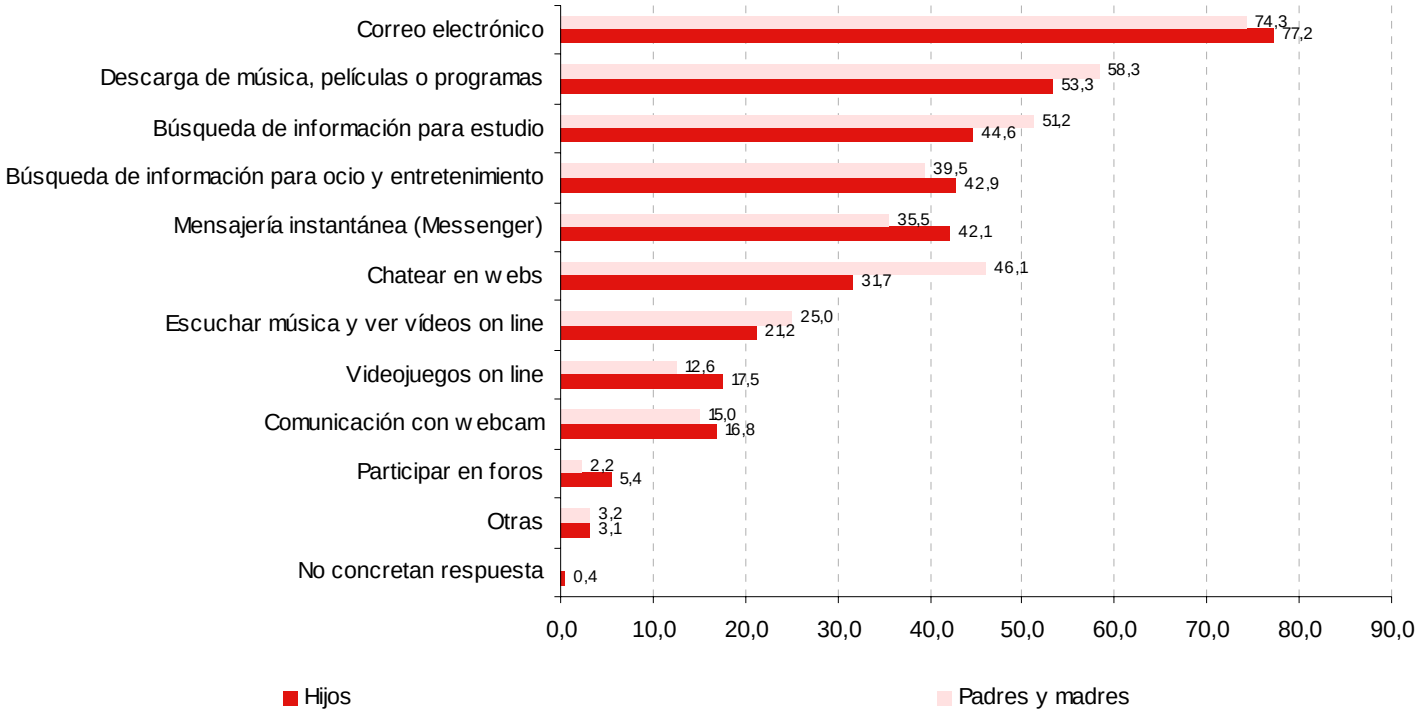


Estudio sobre los hábitos de seguridad en el uso de las TIC de niños y e-confianza de padres y tutores.

Una nueva generación, los *nativos digitales*.

- ✓ Que se conecta todos los días (50%), una media de 1,4 horas (de L a V) y 2,1 horas (S y D)
- ✓ Que declaran que Internet les gusta bastante o mucho más que otras cosas (75%)
- ✓ Que en un 27% de ocasiones navegan solos, sin la presencia de ningún adulto

Servicios de Internet que utiliza el menor (percepción de padres vs. hijos) (%)

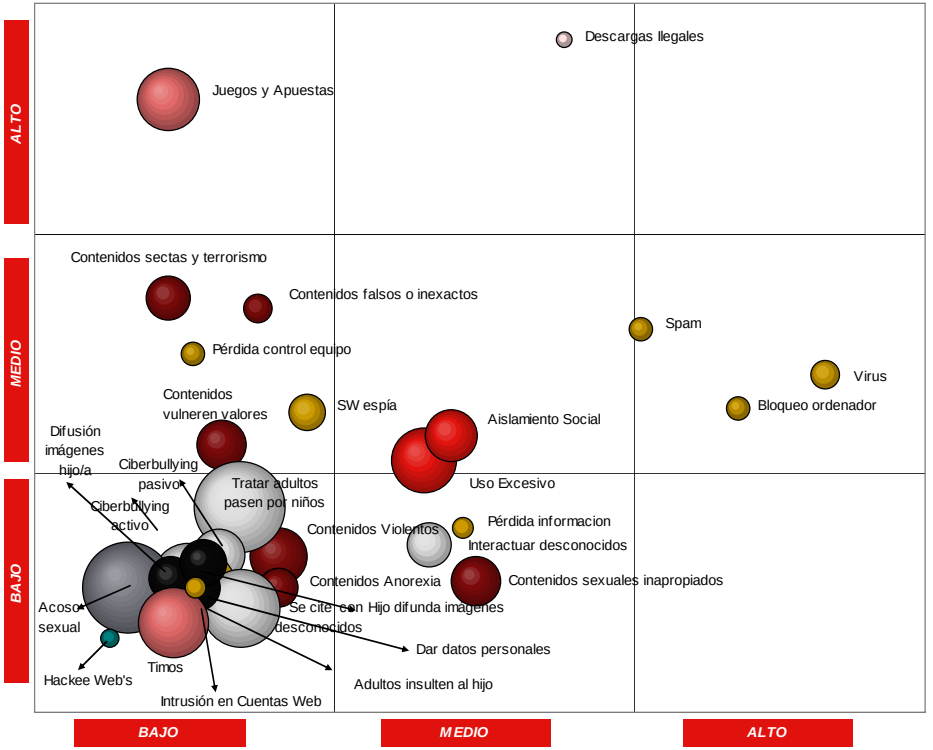


Relación entre impacto (x), frecuencia (y) y gravedad (z)

- Uso abusivo o adicción
- Propiedad industrial o intelectual
- Acceso a contenidos inapropiados
- Cyberbullying y/o acoso
- Grooming y/o acoso sexual
- Amenazas a la privacidad
- Riesgo económico y/o fraude
- Amenazas técnicas y/o malware

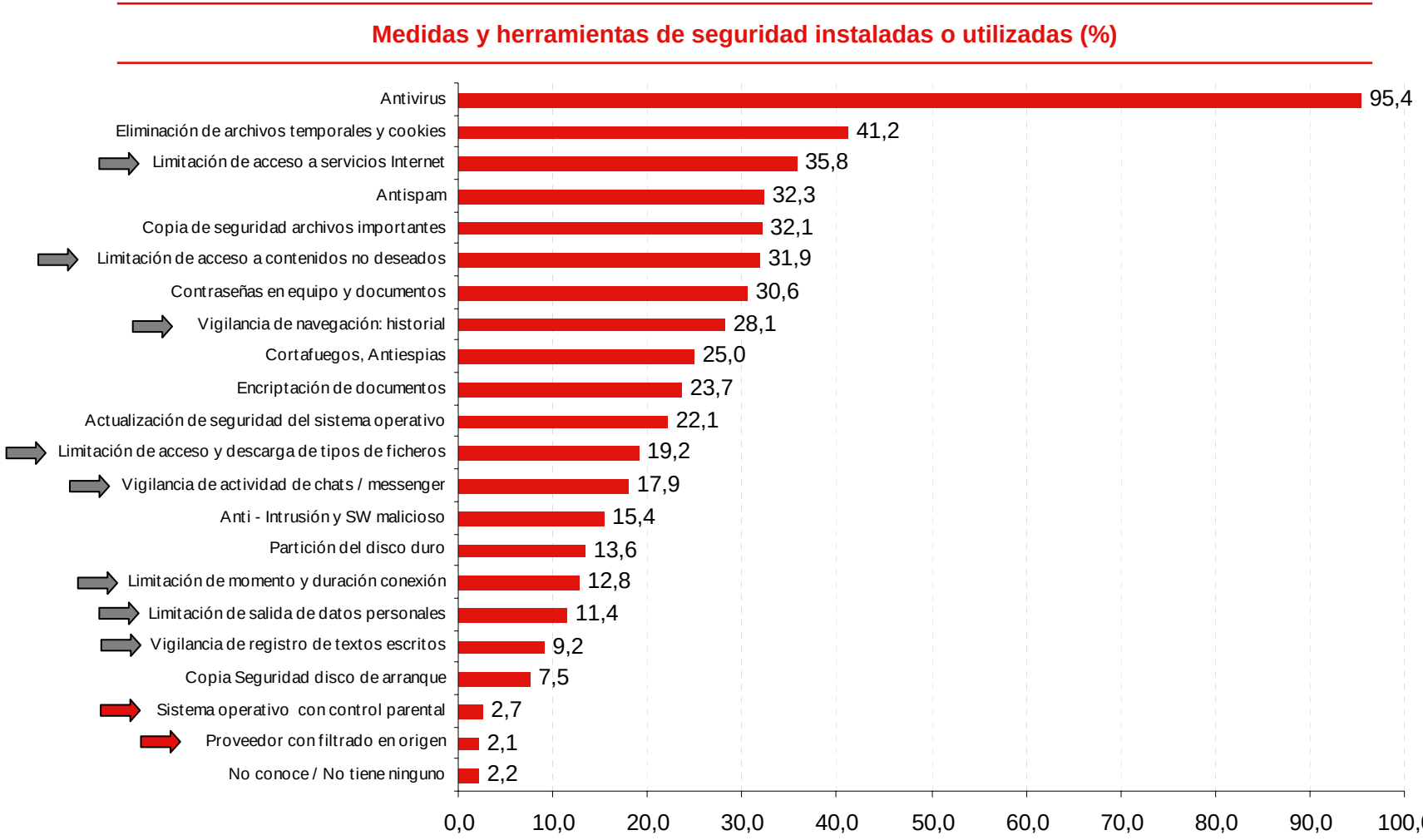
PADRES

HIJOS



Medidas y herramientas de seguridad

Escasa implementación o uso de herramientas y medidas de seguridad específicas para niños y adolescentes.



http://www.inteco.es

http://observatorio.inteco.es