INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

INTECO-CERT

Centro de Respuesta a Incidentes en TI para PYMEs y Ciudadanos

XXIII Grupos de Trabajo RedIRIS

Francisco A. Lago García

26-VI-2007

Contenidos

- **Qué es INTECO**
- **Por qué un CERT para PYMEs y Ciudadanos**
- **INTECO-CERT**

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Instituto Nacional de Tecnologías de la Comunicación

- **Sociedad estatal** adscrita al **MITYC** a través de **SETSI**
- ✓ **Instrumento** para el desarrollo de la Sociedad de la Información
- ✓ **Pilares**: Investigación aplicada, prestación de servicios y formación

INTECO → **OBJETIVOS**

- ✓ **Convergencia** de España con Europa en SI
- ✓ Desarrollar programas de investigación aplicada e innovación en la **SI** y **TIC**
- ✓ Crear en **León** un "Cluster-TIC" con alta capacidad de innovación.
- ✓ **Transversalidad tecnológica** entre sectores y áreas de conocimiento TIC
- ✓ Desarrollar proyectos de contenidos vinculados a un uso intensivo de las TIC
- ✓ Alta localización de **conocimiento intensivo y conexión** con otros centros internacionales.

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Líneas estratégicas de actuación

e-Confianza (Seguridad)

- Centro de Respuesta a Incidentes en TI para PYMEs y Ciudadanos
- Centro Demostrador de Seguridad para la PYME
- Observatorio de Seguridad de la Información

Calidad SW

- Laboratorio Nacional de Calidad
- Formación
- Promoción de proyectos TIC
- Promoción de estándares y normalización

Accesibilidad

- Centro de Referencia en estándares Web
- Promoción de la Accesibilidad Tecnológica y aplicación en la AGE
- Innovación en Tecnologías de Accesibilidad

- Ciudadanía e Internet
- Innovación TIC y Competitividad PYME

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Proyectos en e-Confianza

e-Confianza

- ✓ Sentar las bases de **coordinación de iniciativas públicas** en torno a la seguridad de los SI
- ✓ Coordinar **investigación aplicada y formación especializada** en el ámbito de la seguridad TIC.
- ✓ Convertirse en el **Centro de Referencia** en Seguridad Informática a nivel nacional.

Centro Nacional de Respuesta a Incidentes en TI para PYME y Ciudadanos

Centro Demostrador de Seguridad para la PYME

Observatorio de la Seguridad de la Información

Contenidos

- Qué es INTECO
- Por qué un CERT para PYMEs y Ciudadanos
- INTECO-CERT

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Dificultades específicas PYMEs y Ciudadanos

Falta **conciencia** del problema

Desconocimiento de **productos** y servicios ofrecidos por la industria

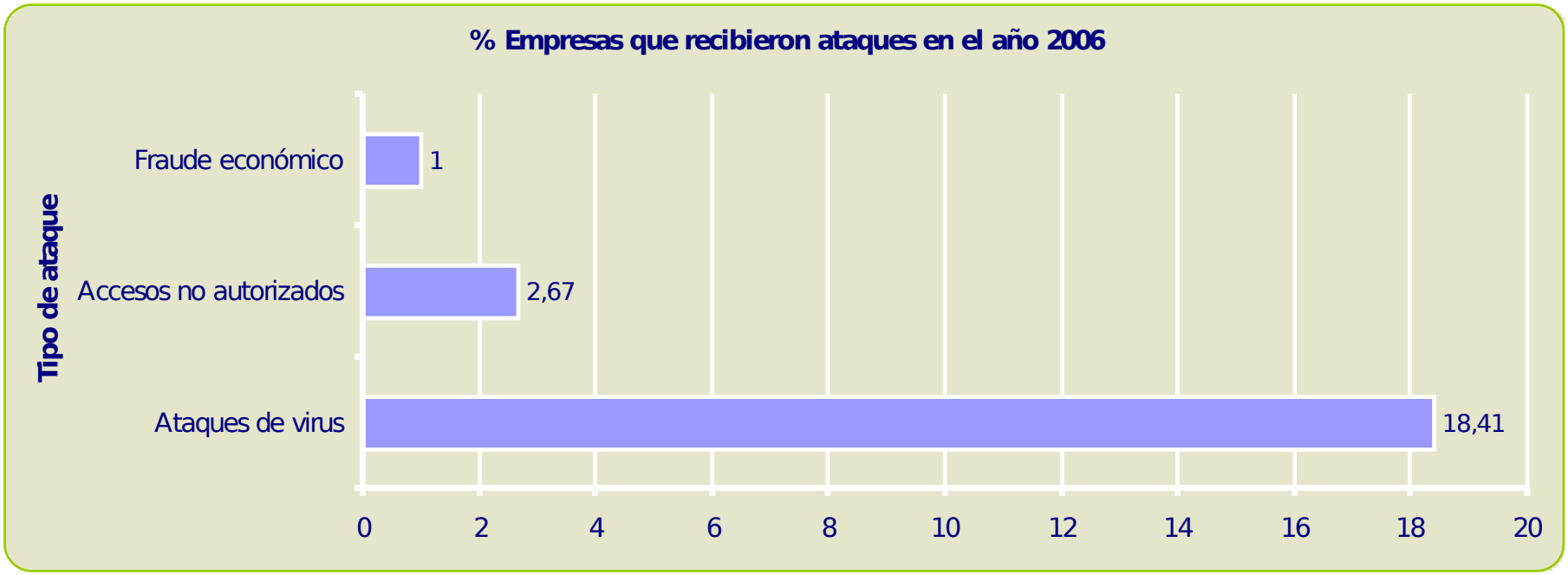
Falta de **personal TIC** y **asesoramiento**

Faltan **productos** o no son **adecuados** a la PYME y Ciudadano

Falta de **formación** en **Seguridad**

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Empresas con ataques



Fuente: INE

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Seguridad de la Información y e-Confianza hogares

- **Observatorio** de la Seguridad de la Información

- **Evaluación** de la **seguridad**, **e-Confianza**, nivel de **incidencias** de seguridad de los hogares españoles usuarios de Internet.
- Universo muestral: **usuarios** de Internet de todas las regiones españolas, edad, género y trabajo.
- **6.357 encuestas** online
- **3.068** equipos domésticos **escaneados**
- Diciembre de 2006 y Enero de 2007
- Próximas oleadas: tendencias y evoluciones

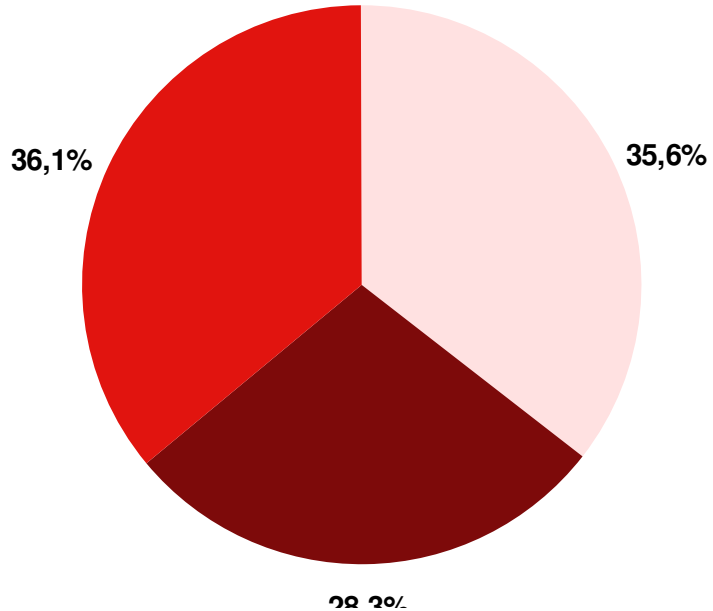
- Informe disponible en: www.inteco.es

Por qué un CERT para PYMEs y Ciudadanos

Dependiendo del tipo de **medidas** utilizadas podemos distinguir sistemas con:

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

Grado de protección de los equipos de los hogares



Por qué un CERT para PYMEs y Ciudadanos

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Medidas de seguridad	*Dispone*	*Previsión para los próximos 3 meses*
Programas antivirus.	94,5	95,8
Cortafuegos	76,0	79,3
Bloqueo de ventanas emergentes	69,5	73,5
Eliminación de archivos temporales y cookies	62,0	68,6
Anti-spam	56,8	64,3
Antiespías	56,8	64,1
Contraseñas (equipo y documentos)	51,6	57,0
Actualizaciones de seguridad del SO	50,1	62,2
Copia de seguridad de archivos importantes	34,2	52,7
Partición del disco duro	31,3	38,3
Copia de seguridad del disco de arranque	22,8	37,3
Programas de control parental	9,2	12,9
Encriptación de documentos	8,5	13,1
Ninguna medida de seguridad	0,7	-

Por qué un CERT para PYMEs y Ciudadanos

INTECO
Instituto Nacional de Tecnologías de la Comunicación

- Los usuarios utilizan **fundamentalmente** medidas de seguridad **automatizadas**.
- Aparece cierto **déficit** en la incorporación de medidas que implican una mayor **proactividad** por parte de los usuarios.

- El **95%** declara poseer un **antivirus** aunque en realidad sólo el **87%** de los panelistas lo tienen **instalado** y activo.
- Las medidas más generalizadas son el **antivirus** y el **cortafuegos**.
- Algo menos del **35%** de los usuarios hacen **copias de seguridad** de sus archivos y menos del **10% encriptan** documentos.
- Las medidas “proactivas” son las que presentan una mayor previsión de crecimiento en los próximos meses.

Por qué un CERT para PYMEs y Ciudadanos

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Medidas de seguridad	No sabe	Innecesario	Precio	Entorpecen	Desconfío	Ineficaces
Programas antivirus.	4,7	24,2	16,7	38,1	5,9	10,4
Cortafuegos	35,7	25,0	8,1	22,6	3,9	4,7
Bloqueo ventanas emergentes	23,7	34,8	8,7	20,9	5,0	6,9
Eliminación archivos temporales y cookies	18,8	59,4	5,2	7,2	3,6	5,8
Anti-spam	14,8	42,5	11,5	12,7	6,7	11,8
Anti-espía	25,7	31,7	11,6	14,5	9,2	7,3
Actualizaciones segur. SO	21,7	47,0	10,2	9,7	6,2	5,2
Contraseñas (equipo y documentos)	8,7	70,6	3,9	8,4	3,1	5,3
Copia seguridad archivos importantes	12,9	67,5	5,3	6,2	2,9	5,2
Partición del disco duro	24,5	56,6	3,8	7,2	3,0	4,9
Copia seguridad disco de arranque	18,4	64,0	4,3	5,9	2,9	4,5
Encriptación de documentos	28,6	56,4	4,3	5,5	3,0	2,2
Programas control parental	9,0	77,3	3,4	4,3	2,1	3,9

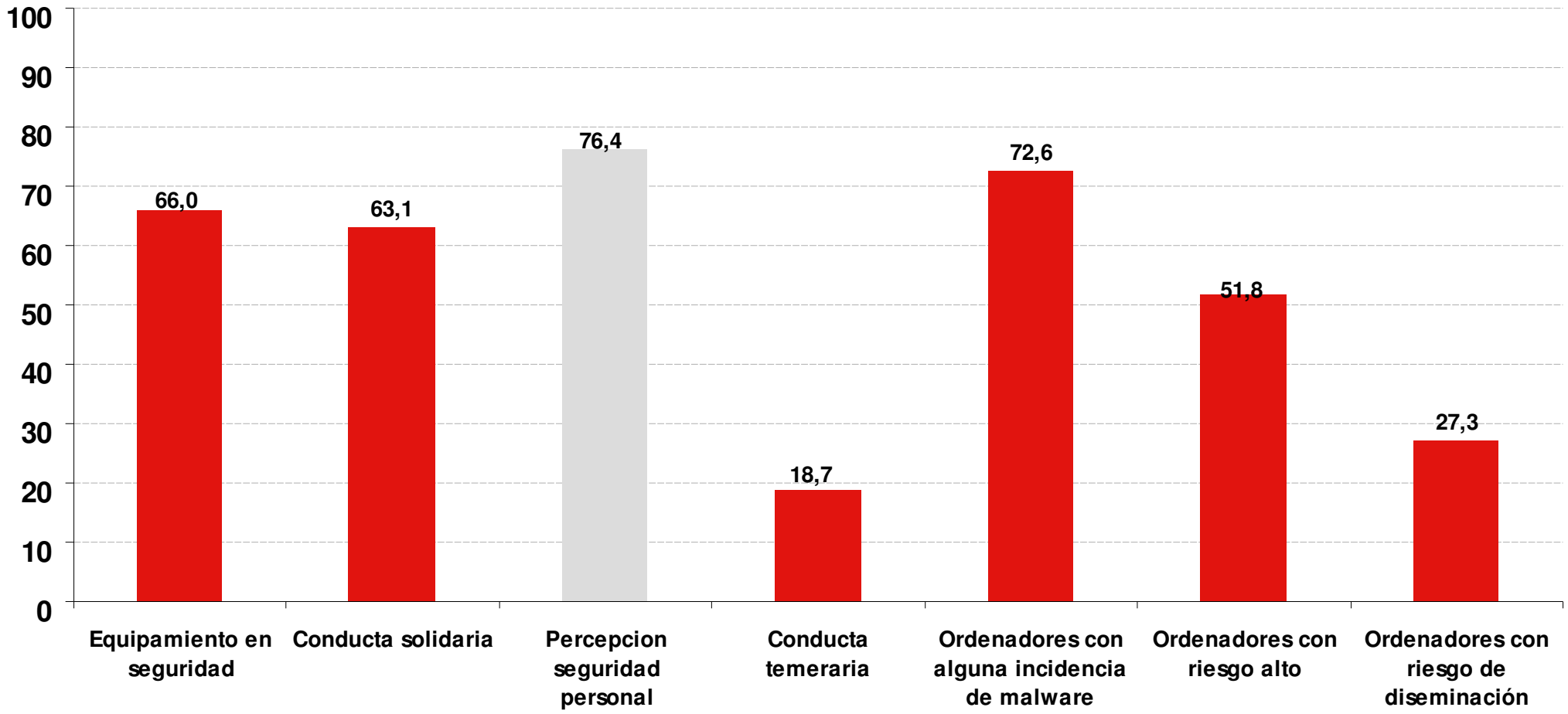
Por qué un CERT para PYMEs y Ciudadanos

INTECO
Instituto Nacional de Tecnologías de la Comunicación

- Los **antivirus**, **cortafuegos** y programas **anti-espía** son las medidas **más valoradas**.
- Las principales **razones** para **no** incorporar las **medidas** de seguridad son:
  - **Desconocimiento** de la medida: hasta un 35,7% en el caso de los cortafuegos.
  - Percepción de que ésta es **innecesaria**: un 24,2% para los antivirus, 25,0% para los cortafuegos y un 31,7% de los que usuarios no utilizan programas anti-espía.
  - Porque consideran que **entorpece** el uso del ordenador y la navegación por Internet: un 38,1% de los panelistas que no usan un antivirus.

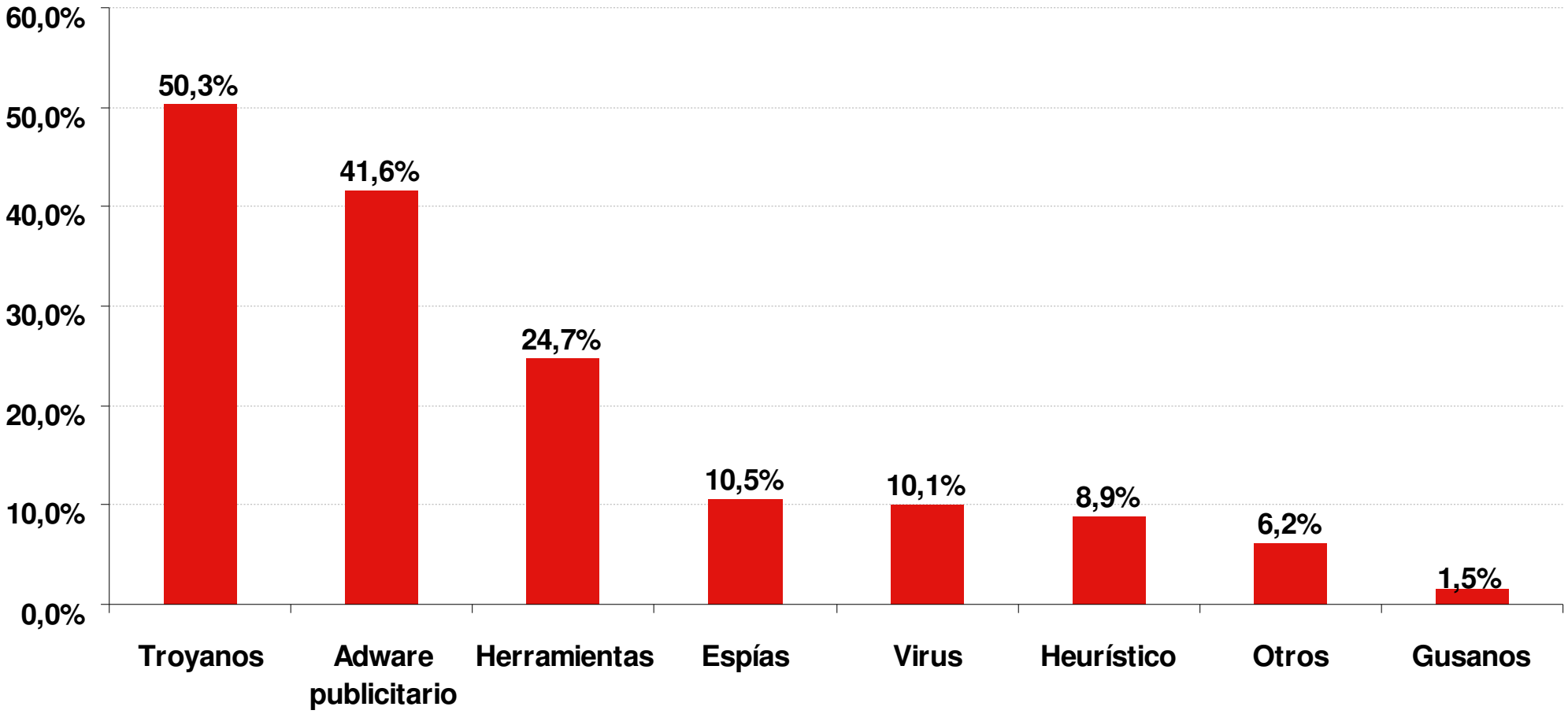
INTECO
Instituto Nacional de Tecnologías de la Comunicación

Sistema de Indicadores de Seguridad y e-Confianza



INTECO
Instituto Nacional de Tecnologías de la Comunicación

Malware Detectado



Por qué un CERT para PYMEs y Ciudadanos

- ✓ El **sistema integral de 7 indicadores sintéticos**, destaca por su carácter sensible, estable, operativo y estratégico.
- ✓ En una **escala de seguridad percibida**: **76,4 puntos** sobre 100 puntos, lo que indica que prevalece una sensación de seguridad bastante extendida.
- ✓ La gran mayoría de los ordenadores tienen malware (72,6 puntos), aunque no todos tienen riesgo alto para los equipos (51,8 puntos) y aún menos riesgo diseminador (27,3 puntos)

- **La seguridad real del sistema tiene origen en dos factores:**
  - Los **hábitos de seguridad** y estilos de uso del ordenador y navegación en Internet.
  - Las **medidas y herramientas** de seguridad instaladas .

Contenidos

- Qué es INTECO
- Por qué un CERT para PYMEs y Ciudadanos
- INTECO-CERT

Objetivos

- Proporcionar **información** clara y concisa acerca de la **tecnología**, su utilización y la **seguridad** que mejore su comprensión.
- **Concienciar** a las PYMEs y ciudadanos de la importancia de contemplar y abordar adecuadamente todos los aspectos relacionados con la **seguridad** informática y de las redes de comunicación
- Proporcionar **guías** de buenas prácticas, **recomendaciones** y precauciones a tener en cuenta para mejorar la seguridad.
- Proporcionar mecanismos y servicios de **divulgación**, **formación**, **prevención** y **reacción** ante incidencias en materia de seguridad de la información.
- Actuar como **enlace** entre las **necesidades** de PYMEs y ciudadanos y las **soluciones** que ofertan las empresas del sector de la seguridad de las tecnologías de la información

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Servicios:

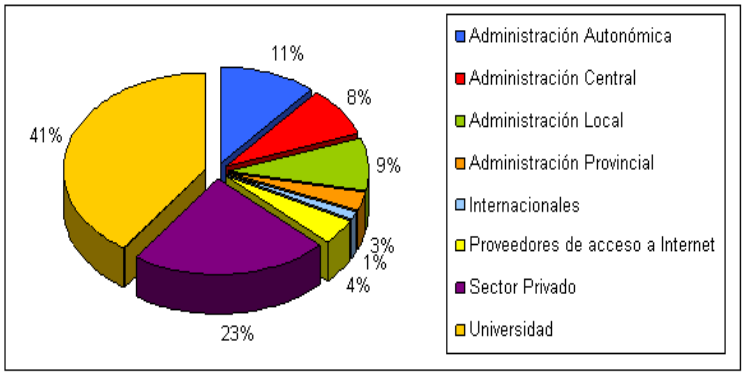
- Servicios de **Suscripción**, mediante el envío de **alertas**, avisos y **boletines** de seguridad.
- Servicios **preventivos**, **reactivos** y correctivos, que incluyen:
  - Gestión y soporte a **incidentes de seguridad**.
  - Gestión de **vulnerabilidades**.
  - Gestión de **malware** y análisis en laboratorio de pruebas.
  - Servicios de **lucha contra el fraude**.
  - **Colaboración** con otras áreas de seguridad de INTECO (Observatorio, Centro Demostrador).
  - **Cooperación y coordinación** con otros agentes del sector tales como las Fuerzas y Cuerpos de Seguridad del Estado, otros Centros de Respuesta a nivel mundial, etc.
- Servicios de **formación** en seguridad para la PYME y ciudadanos.
- Servicios de información y **asesoría** sobre **legalidad** vigente en materia de seguridad en las tecnologías de la información .
- Servicios de **comunicación** y difusión del Centro de Respuesta

Actualmente en producción (CATA)

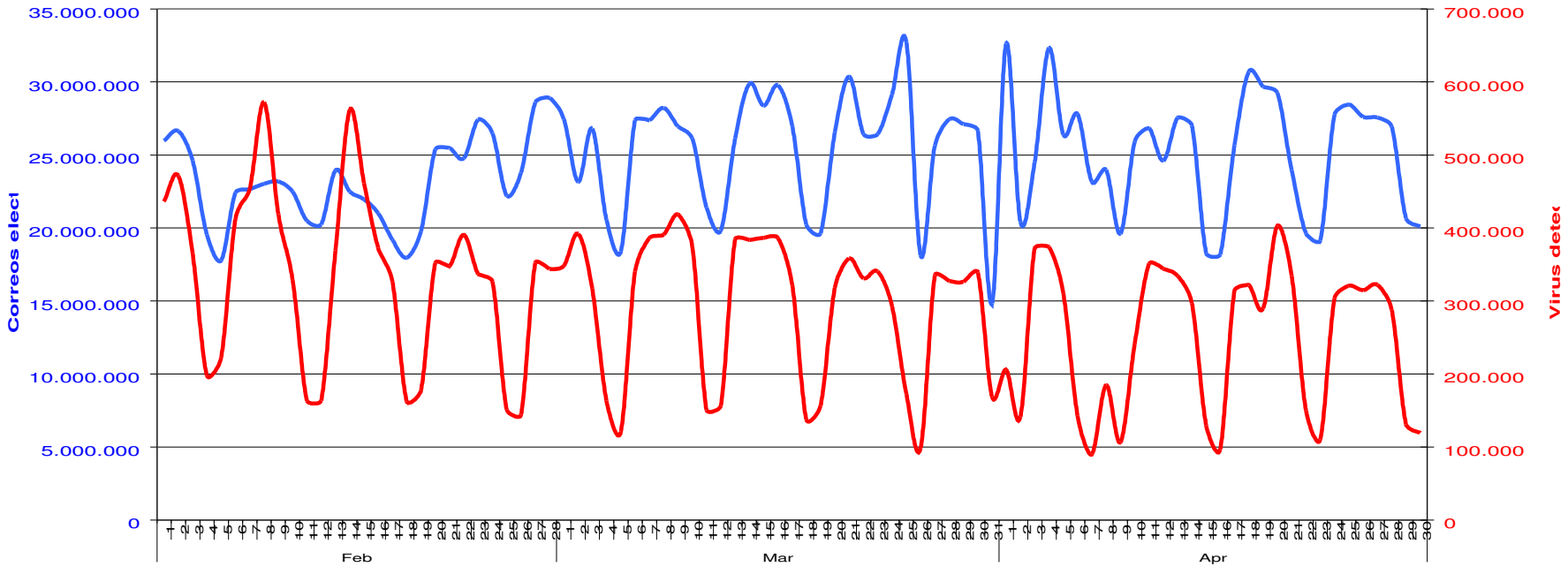
- Desde **2001** referencia en lengua española
- Servicios de **información** y **alertas**:
  - Alertas sobre **virus**
  - **Herramientas** gratuitas
  - Informes diarios
  - Servicio de **suscripción**
  - Foros y buzones
  - Divulgación y formación
  - Información sobre nuevas **vulnerabilidades**

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Red de Sensores



- ✓ Más de **100** sensores → más de **30 millones** de **correos** analizados al día.
- ✓ **4,7%** de detección de correos **infectados** de virus informáticos en más de 11.000 millones de correos analizados.
- ✓ Información de detecciones de malware en correo en www.inteco.es



INTECO
Instituto Nacional de Tecnologías de la Comunicación

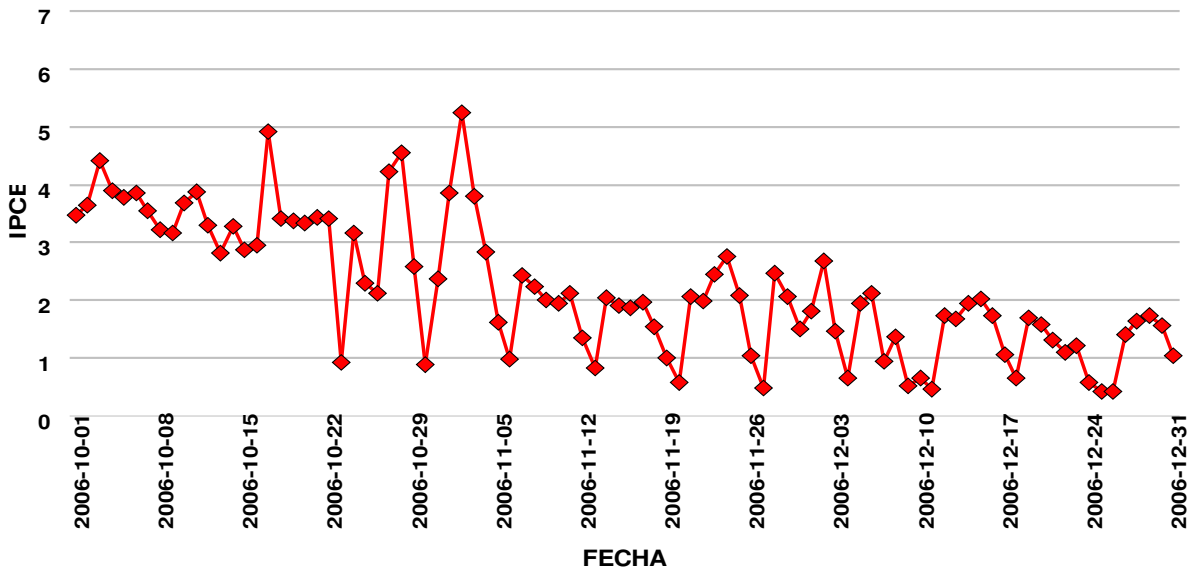
IPCE (Indicador de Peligrosidad del Correo-electrónico)

- ✓ Ofrece diariamente, de forma sencilla, visual y comparable en el tiempo, información sobre el nivel de **peligrosidad** de los **mensajes** de correo electrónico en España (en una escala de 0 a 10).

El IPCE sintetiza diversas variables:

- ✓ **Difusión**
- ✓ **Daño**
- ✓ **Dispersión**
- ✓ **Latencia**

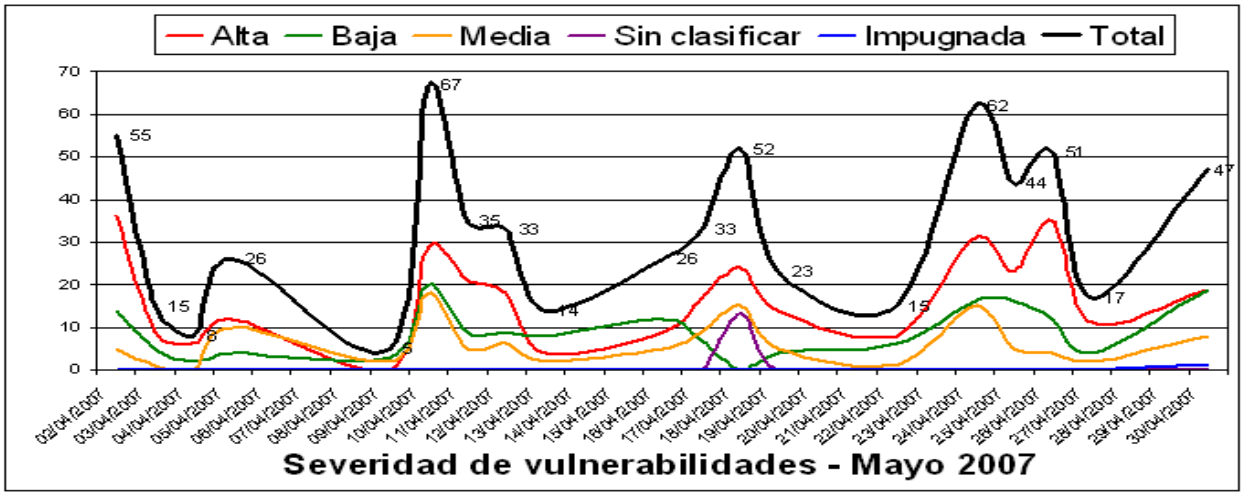
Evolución del IPCE en el último trimestre de 2006



INTECO
Instituto Nacional de Tecnologías de la Comunicación

Información de vulnerabilidades y malware

- ✓ **Vulnerabilidades** descritas en castellano → más de 25.000
- ✓ Clasificación por nivel de **severidad**
- ✓ Actualización diaria
- ✓ Servicio de **suscripción**



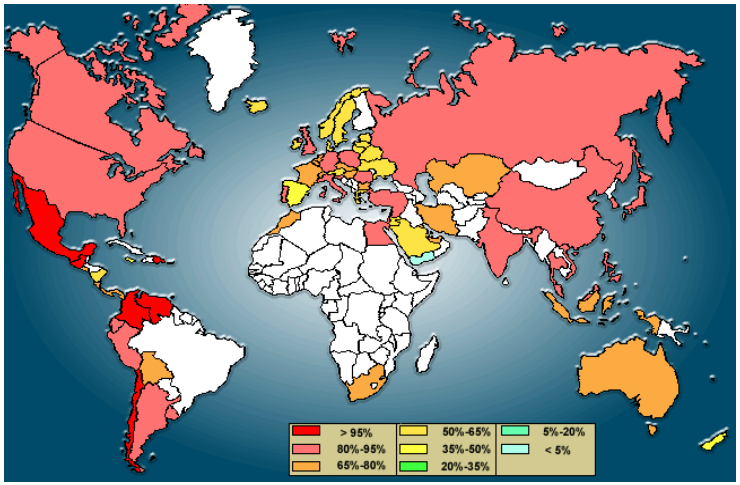
Nombre	Incidencias	Peligrosidad	Descubierto
Netsky.P	101.013 (59,90%)	4 - Alta	22/03/2004
Netsky.Q	23.294 (13,80%)	4 - Alta	29/03/2004
Zafi.D	7.333 (4,40%)	2 - Baja	14/12/2004
Netsky.D	6.263 (3,70%)	2 - Baja	01/03/2004
Netsky.B	5.966 (3,50%)	4 - Alta	18/02/2004

Totales **Muestra**: 31.778.251 **Detecciones**: 168.571
Muestra es el número de mensajes de correo electrónico analizados en la red de sensores
Detecciones es el número de estos mensajes en los que se ha detectado algún virus

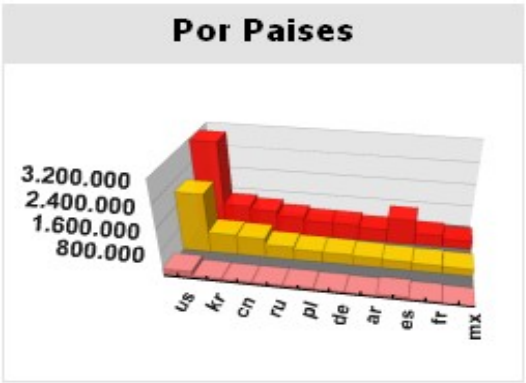
- ✓ Servicio de suscripción a alertas e informes diarios de virus → **250.000 suscriptores**
- ✓ **Información** detallada de virus: 7.000 entradas y 520.000 visitas mensuales
- ✓ Foros de discusión y buzones de consulta
- ✓ Descripción de **herramientas** y útiles gratuitos de ayuda al usuario.

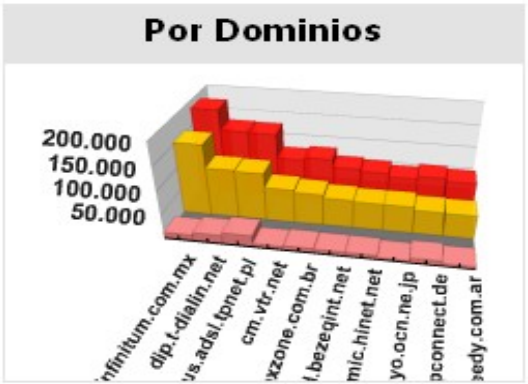
INTECO
Instituto Nacional de Tecnologías de la Comunicación

SANET – Observatorio del SPAM



- ✓ Sensores distribuidos para captura de direcciones IP origen de **SPAM** → análisis del correo emitido desde 1,5 M IP al día
- ✓ Objetivos:
  - ◇ Ampliar datos sobre la **Red de Sensores**.
  - ◇ Estudiar evolución del SPAM y
  - ◇ Relación con distribución de **malware** y **fraude**
  - ◇ Contribuir a la **mejora** del servicio de correo electrónico





CORREOS ELECTRÓNICOS

Rechazados Detectados Procesados

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es