

Seguridad y Alta Disponibilidad: Introducción (I)



IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Alberto Molina Coballes
Jesús Moreno León


Septiembre 2011

Estas diapositivas son una obra derivada de los seminarios de formación impartidos por **Marta Beltrán** y **Antonio Guzmán** de la URJC

© Jesús Moreno León y Alberto Molina Coballes, Septiembre de 2011

Algunos derechos reservados.
Este artículo se distribuye bajo la licencia
"Reconocimiento-CompartirIgual 3.0 España" de Creative
Commons, disponible en
<http://creativecommons.org/licenses/by-sa/3.0/es/deed.es>

Este documento (o uno muy similar)
está disponible en (o enlazado desde)
<http://informatica.gonzalonazareno.org>



Importancia de la seguridad informática

La afirmación de que ahora todo está controlado por computadores es cierta:

- Cuentas bancarias
- Comercio internacional
- Plantas de energía eléctrica
- Ejército
- Satélites
- Sistema judicial
- Sistema sanitario
- ...



Importancia de la seguridad informática

La **Protección** de los sistemas y redes de computadoras es, por tanto, **crítica**

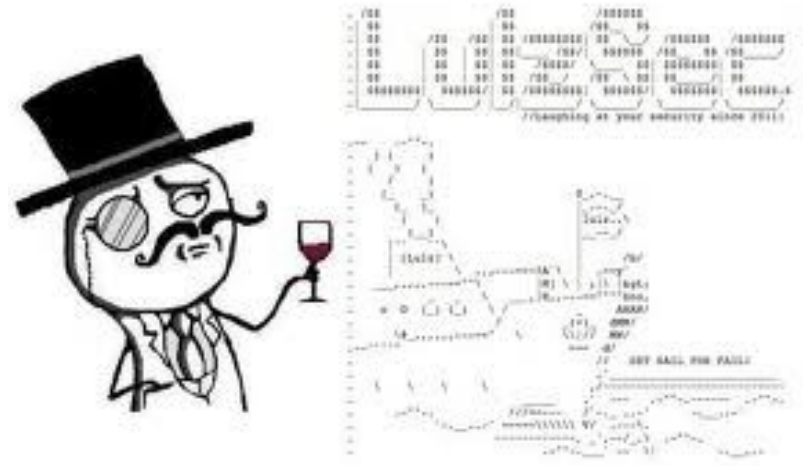
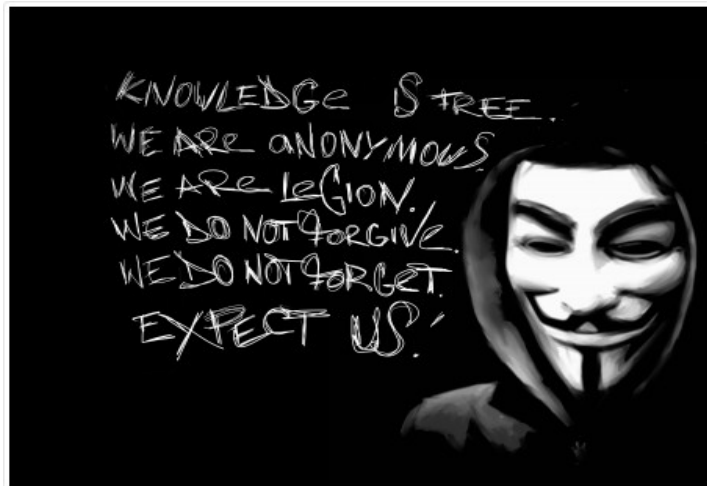
**DESASTRES
ASOCIADOS A
FALLOS
INFORMÁTICOS**



La estrategia actual es adoptar **medidas preventivas** para adelantarse al atacante



Importancia de la seguridad informática



TODAY @ PCWORLD

Sony Gets Hacked Again and Again, Pilfered Data Released

By Ed Oswald, PCWorld Jun 6, 2011 3:30 PM

It's getting a bit old hat, but Sony's been hacked once again. Hacking group Lulzsec, which earlier [had hacked the Sony Pictures website](#), released on Monday some 54 megabytes of source code from Sony's developer network website, as well as network maps from Sony BMG's New York offices.



Definición de seguridad informática

La seguridad informática es:

- El conjunto de servicios y mecanismos que aseguren la **integridad** y **privacidad** de la **información** que los sistemas manejen
- El conjunto de servicios, mecanismos y políticas que aseguren que el **modo de operación** de un sistema sea **seguro**. El que se especificó en la fase de diseño o el que se configuró en tiempo de administración
- El conjunto de protocolos y mecanismos que aseguren que la **comunicación** entre los sistemas esté **libre de intrusos**



Objetivos de la seguridad informática

Confidencialidad

- Garantiza que el acceso a la información no se produce de forma no autorizada

Disponibilidad

- Garantiza que el sistema y los datos estarán disponibles para los usuarios



Objetivos de la seguridad informática

Integridad

- Garantiza que la información no ha sido modificada sin autorización

No repudio

- Impide que el emisor niegue haber estado involucrado en una comunicación



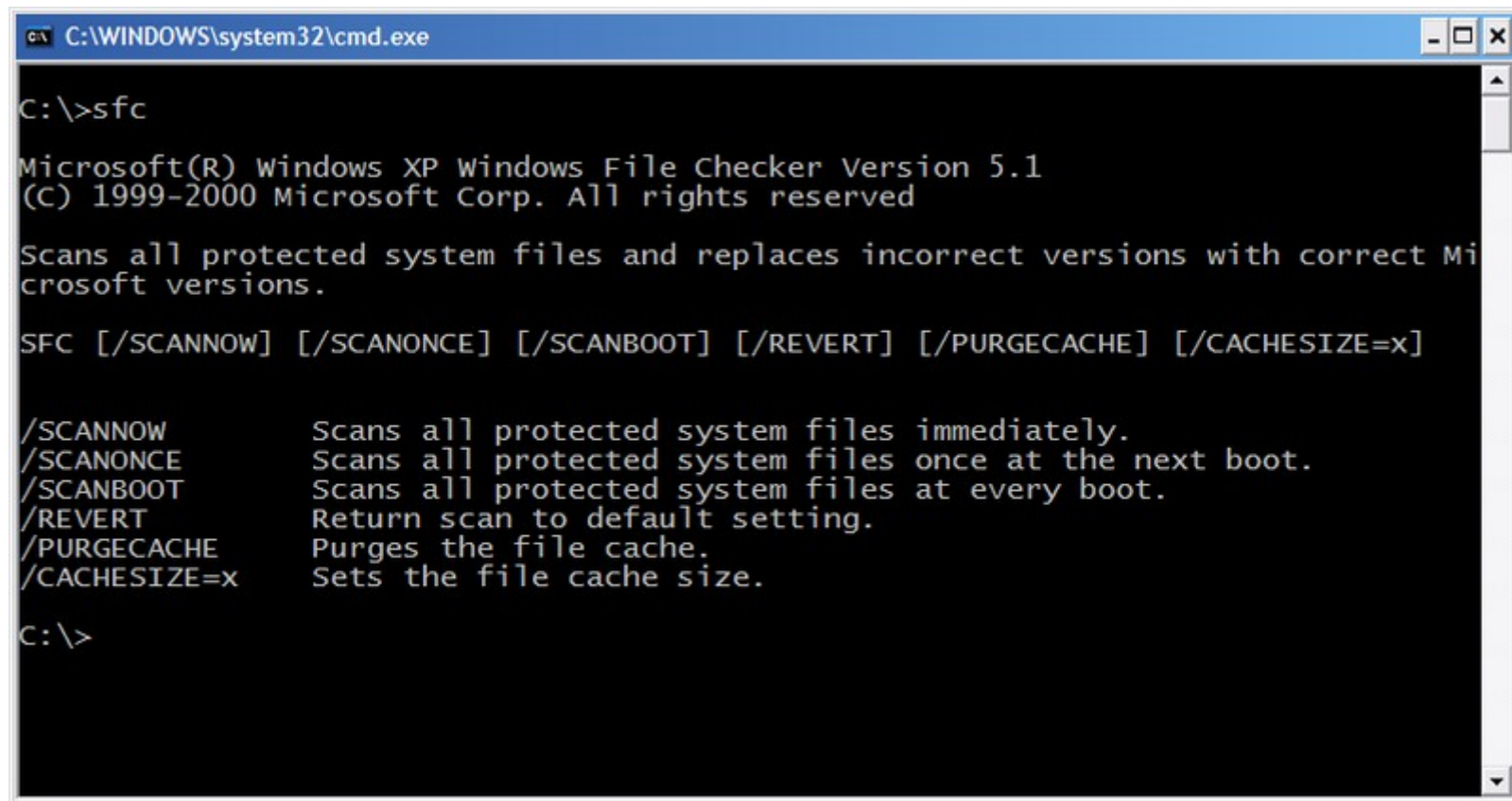
Mecanismos utilizados para conseguir estos objetivos

- Autenticación
- Autorización
- Verificador de integridad de la información
- Cifrado
- Copias de seguridad
- Software anti-malware
- Firewall
- IDS
- Certificados
- Auditoría



Ejercicio: integridad de los archivos del sistema

System File Checker (sfc.exe)



```
C:\WINDOWS\system32\cmd.exe

C:\>sfc

Microsoft(R) Windows XP Windows File Checker Version 5.1
(C) 1999-2000 Microsoft Corp. All rights reserved

Scans all protected system files and replaces incorrect versions with correct Microsoft versions.

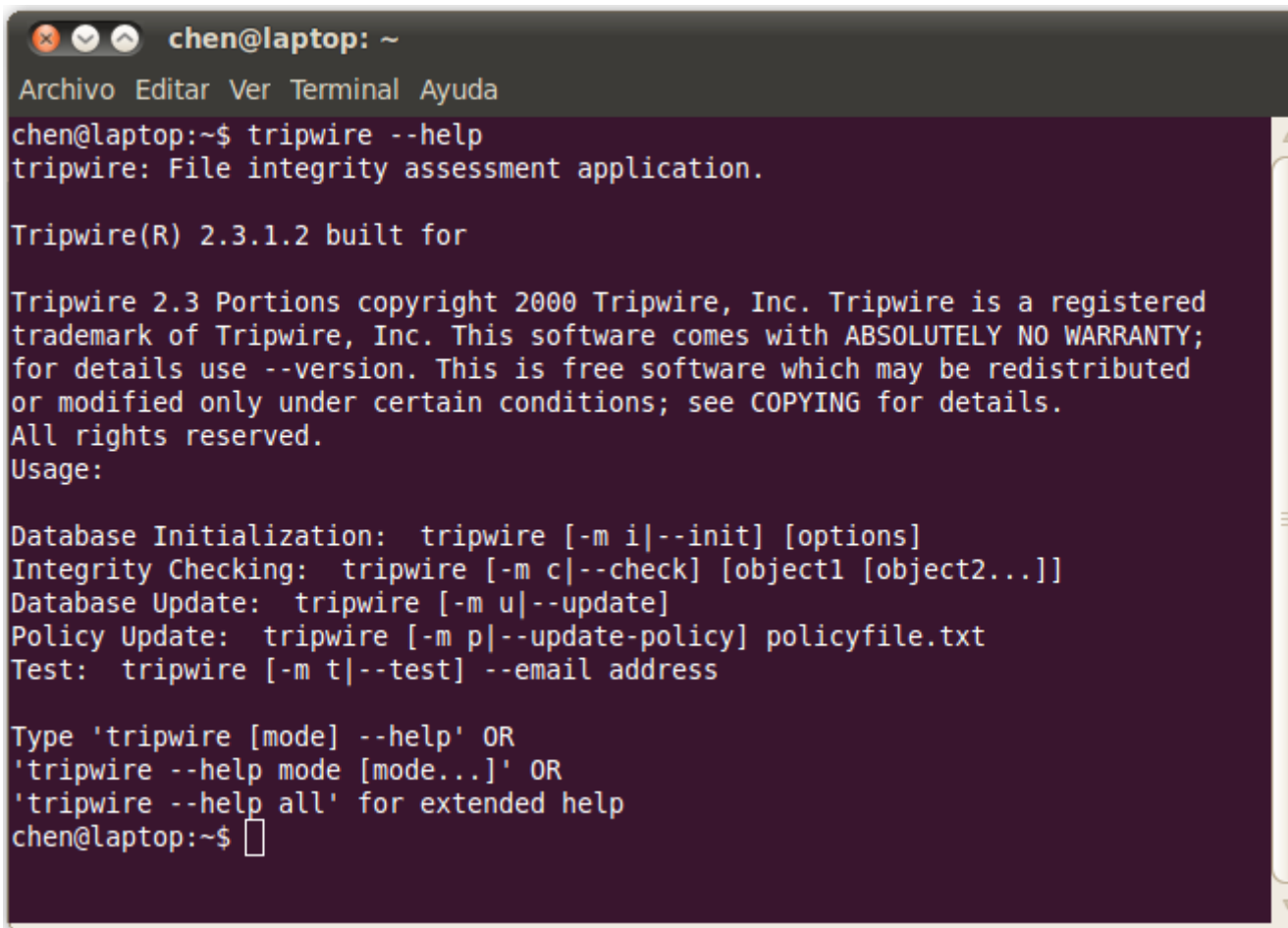
SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE] [/CACHESIZE=x]

/SCANNOW           Scans all protected system files immediately.
/SCANONCE          Scans all protected system files once at the next boot.
/SCANBOOT          Scans all protected system files at every boot.
/REVERT            Return scan to default setting.
/PURGECACHE        Purges the file cache.
/CACHESIZE=x       Sets the file cache size.

C:\>
```

Ejercicio: integridad de los archivos del sistema

- **Tripwire** security and data integrity tool

A screenshot of a terminal window titled 'chen@laptop: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Terminal', and 'Ayuda'. The terminal shows the command 'tripwire --help' and its output. The output describes Tripwire as a file integrity assessment application, version 2.3.1.2, built for Tripwire 2.3. It includes copyright information for Tripwire, Inc. (2000) and states that the software is free but comes with absolutely no warranty. It also lists usage instructions for database initialization, integrity checking, database updates, policy updates, and testing. The prompt 'chen@laptop:~\$' is followed by a cursor.

```
chen@laptop: ~
Archivo Editar Ver Terminal Ayuda
chen@laptop:~$ tripwire --help
tripwire: File integrity assessment application.

Tripwire(R) 2.3.1.2 built for

Tripwire 2.3 Portions copyright 2000 Tripwire, Inc. Tripwire is a registered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
Usage:

Database Initialization: tripwire [-m i|--init] [options]
Integrity Checking: tripwire [-m c|--check] [object1 [object2...]]
Database Update: tripwire [-m u|--update]
Policy Update: tripwire [-m p|--update-policy] policyfile.txt
Test: tripwire [-m t|--test] --email address

Type 'tripwire [mode] --help' OR
'tripwire --help mode [mode...]' OR
'tripwire --help all' for extended help
chen@laptop:~$
```

Alta disponibilidad

Alta disponibilidad (High Availability) es la capacidad de que aplicaciones y datos se encuentre operativos para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter crítico (24 x 7)

Tipo de interrupciones:

- **Previstas:** se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software
- **Imprevistas:** suceden por acontecimientos imprevistos (apagón, error de hardware/software, problemas de seguridad, desastre natural, virus, ...)



Clasificación de la seguridad informática

FÍSICA



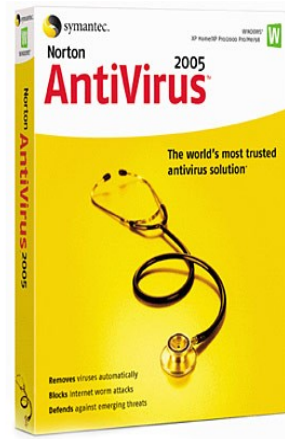
ACTIVA



VS

VS

LÓGICA

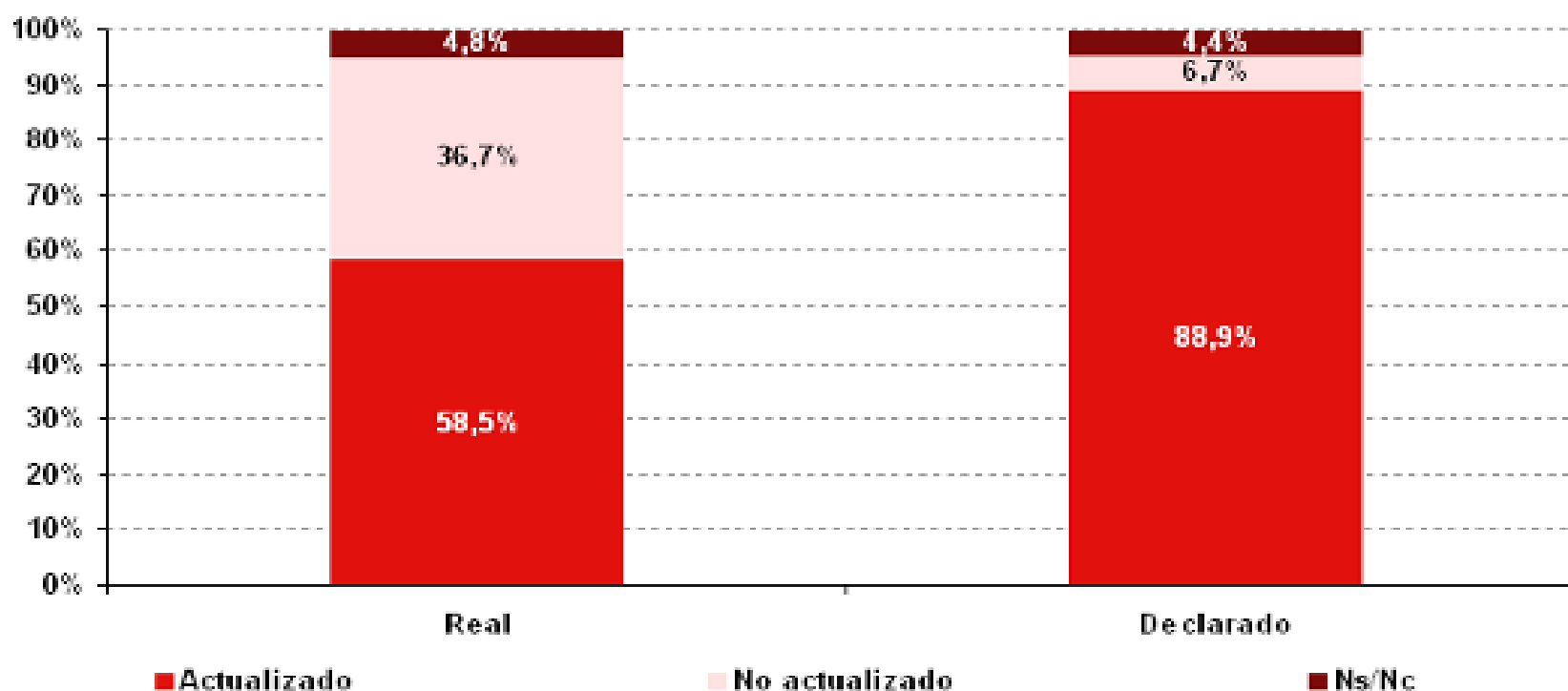


PASIVA



Déficit de formación en técnicos y usuarios

Estado de actualización del sistema operativo y de las herramientas de seguridad de las empresas: datos declarados vs. datos reales (%)

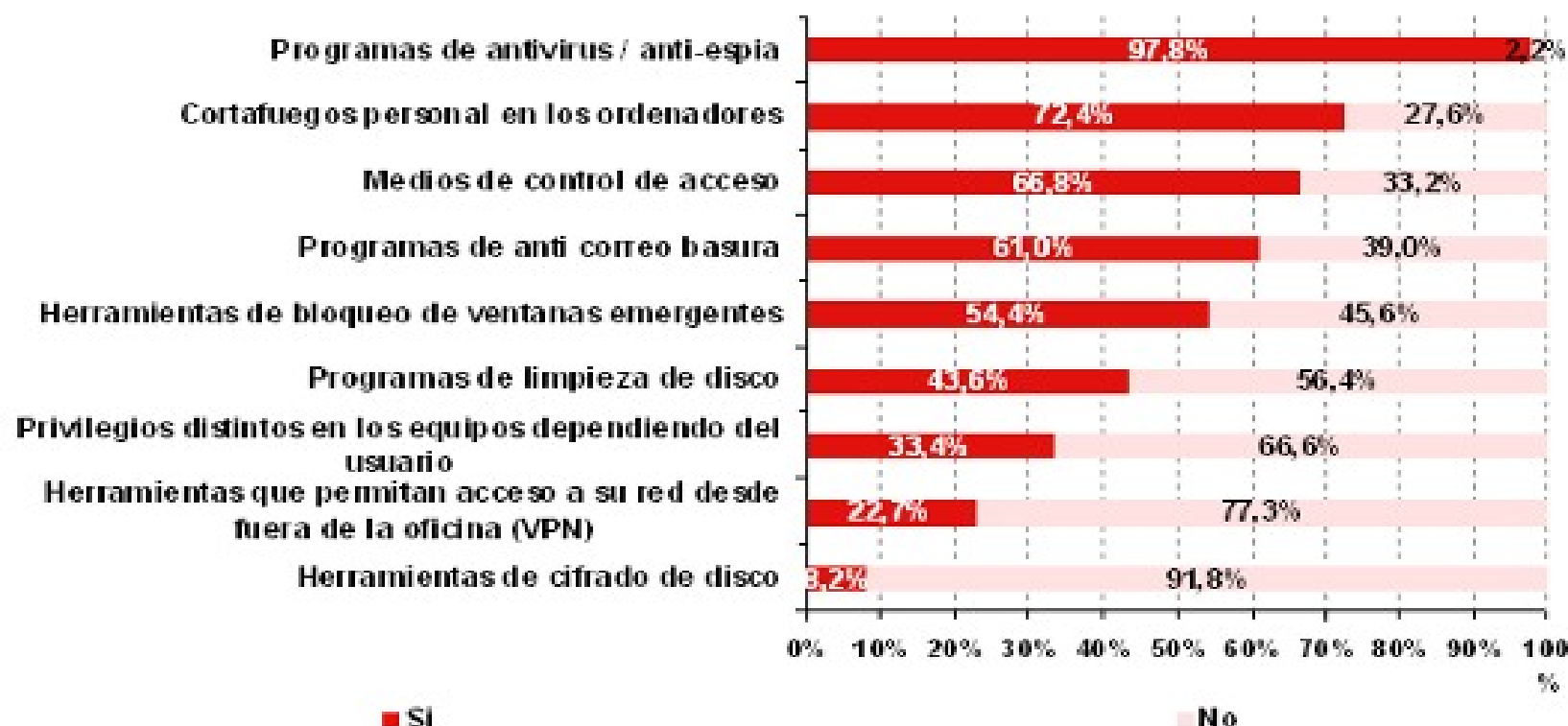


Declarado n=2.206, Real n=622

Fuente: INTECO

Déficit de formación en técnicos y usuarios

Nivel de implantación de las soluciones de seguridad en los ordenadores de la entidad (%)



n=2.206

Fuente: INTECO

Déficit de formación en técnicos y usuarios

Motivos aducidos para no aplicar las medidas de seguridad (%)

Medidas de seguridad	No sé lo que es	Porque innecesario es	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 seguridad 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 parental control	9,0	77,3	3,4	4,3	2,1	3,9

Ejercicio: test sobre seguridad informática

Vamos a probar nuestros conocimientos sobre seguridad informática con un test (muy básico) de la Oficina de Seguridad del Internauta:

